THE UNIVERSITY OF CHICAGO
SCIENCE SERIES

The University of Chicago Science Series, established by the Trustees of the University, owes its origin to a feeling that there should be a medium of publication occupying a position between the technical journals with their short articles and the elaborate treatises which attempt to cover several or all aspects of a wide field. The volumes of the series will differ from the discussions generally appearing in technical journals in that they will present the complete results of an experiment or series of investigations which previously have appeared only in scattered articles, if published at all. On the other hand, they will differ from detailed treatises by confining themselves to specific problems of current interest, and in presenting the subject in as summary a manner and with as little technical detail as is consistent with sound method.

FINITE COLLINEATION GROUPS

THE UNIVERSITY OF CHICAGO PRESS
CHICAGO, ILLINOIS

Agents

THE BAKER & TAYLOR COMPANY
NEW YORK

THE CUNNINGHAM, CURTISS & WELCH COMPANY
LOS ANGELES

THE CAMBRIDGE UNIVERSITY PRESS
LONDON AND EDINBURGH

THE MARUZEN-KABUSHIKI-KAISHA
TOKYO, OSAKA, KYOTO, FUKUOKA, SENDAI

THE MISSION BOOK COMPANY
SHANGHAI

FINITE COLLINEATION GROUPS

WITH AN INTRODUCTION TO THE THEORY
OF GROUPS OF OPERATORS AND
SUBSTITUTION GROUPS

By

H. F. BLICHFELDT

Professor of Mathematics in Leland Stanford Junior University

THE UNIVERSITY OF CHICAGO PRESS
CHICAGO, ILLINOIS

Published April 1917

Composed and Printed By
The University of Chicago Press
Chicago, Illinois, U.S.A.

PREFACE

The theory of finite collineation groups (or linear groups) as developed at present is to be found mainly in scattered articles in mathematical journals, in addition to a few texts on group theory. The author has endeavored in the present volume to give an outline of the different principles contained in these publications, and has at the same time made an effort to depend upon a minimum of abstract group theory. In this and many other respects the present volume differs from Part II of the last book cited in § 24; in particular, the present volume contains more of the theory of linear groups, though the student is referred to that Part II for lists of the invariants of the binary and ternary groups.

No previous knowledge of the technique of group theory is required for the reading of the opening chapter, which develops the fundamental properties of linear transformations and linear groups. For the greater convenience of the student, an introduction to the theory of groups of operators and substitution groups is given in the second chapter; moreover, certain theorems and definitions from the more advanced parts of algebra needed throughout the book are stated in explicit form in an Appendix.

The groups in two variables are determined in chap. iii by a modified form of a process due to Klein, which depends largely upon geometrical intuition. Theorems which serve as a means for determining the relatively difficult linear groups in more than two variables are presented in chap. iv, and are, in fact, made use of in

the chapters on ternary and quaternary groups (chaps. v and vii).

Concerning the theory of group characteristics (chap. vi), an attempt has been made to exhibit this subject in a very simple form, by means of explicit definitions and easy proofs which eliminate complicated sigma-constructions. The student is here (as elsewhere) urged to work with the matrix form of a linear transformation and intransitive group (§§ 2, 85).

Where purely geometrical methods are not available or are less convenient than analytical methods, collineation groups are most easily studied through the medium of "linear groups" (cf. §§ 10, 51); hence the almost exclusive discussion of the latter category in the text.

The author owes his thanks to his colleagues, Professors R. E. Allardice and W. A. Manning, for the care with which they have read the manuscript and for many helpful criticisms. He is also deeply indebted to Professors E. H. Moore and L. E. Dickson of the University of Chicago for their generous encouragement and valuable suggestions.

H. F. Blichfeldt

Leland Stanford Junior University

TABLE OF CONTENTS

CHAPTER I

ELEMENTARY PROPERTIES OF LINEAR GROUPS

LINEAR TRANSFORMATIONS: FUNDAMENTAL PROPERTIES, §§ 1–6

1. **Examples of linear transformations.—Operator.** Let the axes of co-ordinates (rectangular) in the plane be rotated through an angle θ, the origin remaining fixed. If x, y are the co-ordinates of any given point with reference to the axes in their original position, and x', y' the co-ordinates of the same point with reference to the axes in their new position, then, as is proved in analytic geometry,

$$\begin{aligned} x &= x' \cos\theta - y' \sin\theta, \\ y &= x' \sin\theta + y' \cos\theta. \end{aligned} \tag{1}$$

Hence, if a given curve has for its equation

$$f(x, y) = 0 \tag{2}$$

with reference to the old axes, then its equation with reference to the new axes will be

$$f(x' \cos\theta - y' \sin\theta,\ x' \sin\theta + y' \cos\theta) = 0. \tag{3}$$

We shall say that (3) is obtained from (2) by the *linear transformation* (1). In conformity with the general group terminology we call the transformation (1) an *operator*, which, *operating* upon (2), produces (3).

To take a second example: any literal substitution (cf. chap. ii, B) can be exhibited as a linear transformation. For instance, the substitution $(x_1x_2x_3)(x_4x_5)$ can be written

$$x_1 = x_2',\ x_2 = x_3',\ x_3 = x_1',\ x_4 = x_5',\ x_5 = x_4'.$$

2. **Formal definition.** *A linear transformation in n variables is a set of linear homogeneous equations,*

$$
\begin{aligned}
x_1 &= a_{11}x_1' + a_{12}x_2' + \ . \ . \ . \ + a_{1n}x_n' \ , \\
x_2 &= a_{21}x_1' + a_{22}x_2' + \ . \ . \ . \ + a_{2n}x_n' \ , \\
&\ . \quad . \quad . \quad . \quad . \quad . \quad . \\
x_n &= a_{n1}x_1' + a_{n2}x_2' + \ . \ . \ . \ + a_{nn}x_n' \ ,
\end{aligned} \tag{4}
$$

expressing the original variables $x_1, \ . \ . \ . \ , x_n$ in terms of new variables $x_1', \ . \ . \ . \ , x_n'$, under the condition that the equations can be solved for the latter; that is, the determinant of the coefficients a_{st} $(s, t = 1, 2, \ . \ . \ , n)$, called the *determinant of the transformation*, must not vanish.

We represent a linear transformation by a capital letter (as A, S, . .), or, if we wish to be specific, by the *matrix of the linear transformation*

$$
\begin{bmatrix}
a_{11} & a_{12} & . & . & a_{1n} \\
. & . & . & . & . \\
a_{n1} & a_{n2} & . & . & a_{nn}
\end{bmatrix}
$$

which may be abbreviated to $[a_{st}]$. Thus the equation $A = [a_{st}]$ implies that a transformation denoted by A has for coefficients the numbers a_{st} $(s, t = 1, 2, \ . \ . \ , n)$. The same implication is also indicated by writing $A:$ to the left of the equations (4). The equation $A = B$ is equivalent to the statement that the matrices of A and B are identical.

We do not a priori place any restrictions on the form of the numbers a_{st}. They may be real or imaginary, rational or irrational.

The transformation (4), which we shall denote by A, operates upon a given function $f(x_1, \ . \ . \ , x_n)$ by putting in place of $x_1, \ . \ . \ , x_n$ the equivalent expressions in the right-hand members of (4). This is indicated symboli-

cally by $(f)A$. However, for reasons apparent later, we shall *drop the accents* after the operation has been performed. Thus, if S is the transformation (1) and f the function (2), the left-hand member of the equation (3) will be written

$$(f)S=f(x\cos\theta-y\sin\theta,\ x\sin\theta+y\cos\theta)$$

in the future.

Certain special forms of linear transformations occur frequently or are introduced for convenience:

(*a*) *Canonical form.*—If every $a_{st}=0$ in (4) except when $s=t$, we say that A has the *canonical form.* In this case we write $A=(a_{11}, a_{22}, \ldots, a_{nn})$. The coefficients $a_{11}, a_{22}, \ldots, a_{nn}$ are here called the *multipliers* of A.

The transformations A_2, E, B_2, B_4, § 7, all have the canonical form.

(*b*) *Similarity-transformation.*—This is a transformation in canonical form all of whose multipliers are equal $(a_{11}=a_{22}=\ \ldots\ =a_{nn})$, as in the cases A_2, E, § 7.

(*c*) *The identity.*—This is a similarity-transformation whose multipliers are unity.

We shall reserve the letter E for this transformation: $E=(1, 1, \ldots, 1)$. Evidently, the identity produces no change; that is, $(f)E=f$. For an illustration, put $\theta=0$ in (1).

3. **The product of linear transformations.** If we operate on a given function f by two linear transformations successively, say first by A and then by B, the result, which is written $(f)AB$, is equivalent to that obtained by operating on f by a single linear transformation C. For instance, let f be a function $f(x, y)$, A the transformation (1), § 1, and $B=(a, b)$, and we find

$$(f)AB=f(xa\cos\theta-yb\sin\theta,\ xa\sin\theta+yb\cos\theta),$$

which is obviously also the result of operating on $f(x, y)$ by

$$C: \quad x = x'a \cos\theta - y'b \sin\theta, \quad y = x'a \sin\theta + y'b \cos\theta.$$

Remark.—We notice that

$$(f)BA = f(xa \cos\theta - ya \sin\theta, \; xb \sin\theta + yb \cos\theta),$$

so that $(f)AB \neq (f)BA$ unless $(a-b) \sin\theta = 0$.

THEOREM 1. *Let $A = [a_{st}]$ and $B = [b_{st}]$ be two linear transformations in n variables. Operating first by A and then upon the result by B is equivalent to operating originally by a single linear transformation $C = [c_{st}]$ in n variables, where*

$$(5) \qquad c_{st} = a_{s1}b_{1t} + a_{s2}b_{2t} + \ . \ . \ + a_{sn}b_{nt} = \sum_{k=1}^{n} a_{sk}b_{kt}$$
$$(s, t = 1, 2, \ . \ . \ , n).$$

*We say that C is the product of A and B, and write symbolically $AB = C$.**

The rule for finding the product $AB = C$ may be described in the following manner (*matrix multiplication*). We define the product of a row (horizontal) of A, say $a_{21}, a_{22}, \ . \ . \ , a_{2n}$, and a column (vertical) of B, say $b_{13}, b_{23}, \ . \ . \ , b_{n3}$ as follows: multiply the first element of the row by the first element of the column, the second element of the row by the second element of the column, etc., and add the resulting n products $(a_{21}b_{13} + a_{22}b_{23} + \ . \ . \ + a_{2n}b_{n3}$ in the

* A value for c_{st} different from that given above is obtained by writing last in the product that transformation which operates first, as is the custom with functional operators $(BA(f))$, or by regarding the accented letters in (4), § 2, as the old variables and the unaccented as the new. Thus, Klein, Jordan, Burnside, and Weber obtain

$$c_{st} = \Sigma_{k=1}^{k=n} a_{ks}b_{tk},$$

while Schur and Frobenius get the value given in (5). The author has hitherto (in papers published in technical journals) accented the old and left unaccented the new variables, and has used the term "linear substitution" for "linear transformation."

example). Then c_{st} is the product of the sth row of A and the tth column of B.

The value of c_{st} given above is found by eliminating $x_1', x_2', \ldots, x_n'$ from the two sets of equations

$$A: \; x_s = a_{s1}x_1' + \ldots + a_{sn}x_n',$$
$$B: \; x_s' = b_{s1}x_1'' + \ldots + b_{sn}x_n'' \qquad (s = 1, 2, \ldots, n).$$

4. **The commutative and associative laws. Power of a linear transformation.** In general, the commutative law does not hold; that is, AB differs from BA (cf. *Remark*, § 3). On the other hand, the associative law holds in a product of three or more transformations. Thus, let A, B, C be any three transformations, and let $AB = P$ and $BC = Q$. Then $(AB)C = PC = AQ = A(BC)$. As a consequence the notation ABC is not ambiguous, and we shall write A^2 for AA, A^3 for A^2A, etc. We call A^m the mth *power* of the transformation A.

To prove the associative law, we construct the matrices of $P = [p_{st}] = AB$, $Q = [q_{st}] = BC$ by Theorem 1, § 3, and then those of PC and AQ.

Linear transformations having the canonical form are commutative and their products are readily written down. In particular, if

$$S = (a_{11}, a_{22}, \ldots, a_{nn}), \; T = (b_{11}, b_{22}, \ldots, b_{nn}),$$

we have

$$ST = TS = (a_{11}b_{11}, a_{22}b_{22}, \ldots, a_{nn}b_{nn}),$$

and

$$S^m = (a_{11}^m, a_{22}^m, \ldots, a_{nn}^m).$$

5. **The inverse of a linear transformation S** is such a transformation, written S^{-1}, that the product SS^{-1} is equivalent to the identity E; i.e., produces no final change. In the case of the transformation (1), § 1, the inverse is

plainly the rotation of the axes through the angle $-\theta$: $x=x' \cos \theta+y' \sin \theta$, $y=-x' \sin \theta+y' \cos \theta$. It is also plain that, having transformed a function $f(x, y)$ by means of (1) into a function $F(x', y')$, we get the original function $f(x, y)$ by substituting in F the values of x', y' expressed in terms of x, y. These solutions appear in the form of a linear transformation after the accents have been properly placed.

THEOREM 2. *The inverse of a linear transformation S:*

$$x_s=a_{s1}x'+ \ . \ . \ +a_{sn}x'_n \quad (s=1, 2, \ . \ . \ , n),$$

is obtained by solving this system of linear equations for x'_1, x'_2, . . . , x'_n *in terms of* x_1, x_2, . . . , x_n. *After the accents have been properly placed, these solutions appear in the standard form of a linear transformation, denoted by* S^{-1}.

More generally, we shall denote the inverse of S^m by S^{-m}, and we have $S^mS^{-m}=S^{-m}S^m=E$.

We can now prove that, given $AB=AC$, then $B=C$. For, from $A^{-1}(AB)=A^{-1}(AC)$ follows (§ 4):

$$(A^{-1}A)B=B=(A^{-1}A)C=C.$$

Similarly, if $BA=CA$, then $B=C$.

6. **Order of a linear transformation.** Consider the transformation (1), § 1, which we shall indicate by S. If θ is an aliquot part of 2π, then some power of this transformation will be equivalent to the identity. Thus, if θ is a right angle, $S^4=E$. In general, if S is an arbitrarily chosen transformation, the identity will *not* be found among the powers of S. If it should be, we say that S is of *finite order;* and if m is the lowest positive integer for which $S^m=E$, we say that S *is of order* m. In this case no power of S need be taken higher than m.

For, since $S^{m+a}=S^mS^a$, and the operator S^m produces no change, it follows that $S^{m+a}=S^a$.

If S is of order m, the order of S^k is m/d, where d is the highest common factor of m and k (cf. § 26, (*b*)). Thus, if $m=12$, then S^5, S^7 and S^{11} are of order 12; S^4 and S^8 of order 3, and so on.

Exercises

1. If d_1 and d_2 are the determinants of the linear transformations A_1 and A_2 in two variables, then the determinant of A_1A_2 is d_1d_2.

2. Prove that the product of a linear transformation T and a similarity-transformation $S=(a, a, \ldots, a)$ is obtained by merely multiplying every element in the matrix of T by a.

Hence prove that a similarity-transformation is commutative with every transformation in the same variables.

3. Find the general form of a linear transformation in three variables which is commutative with $S=(a, a, b)$.

4. Prove that the two transformations

$$A=\begin{bmatrix} p & q \\ r & s \end{bmatrix}, \qquad B=\begin{bmatrix} s & -q \\ -r & p \end{bmatrix}, \qquad ps-qr=1,$$

are each the inverse of the other.

5. If S is of order m, then S^{m-1} is the inverse of S.

6. A linear transformation is the inverse of its own inverse.

7. Are the following transformations of finite order:

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \qquad \begin{bmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{bmatrix}, \qquad \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix} ?$$

8. Prove that the multipliers of a transformation of finite order are *roots of unity* (cf. § 133).

GROUPS OF LINEAR TRANSFORMATIONS: CLASSIFICATION, CHANGE OF VARIABLES, §§ 7–14

7. Finite groups of linear transformations. Let there be given a set of distinct linear transformations, finite in number, and let it be known that the product of any two

of the set (AB as well as BA), whether alike or distinct, is again a transformation of the set; then this set is called *a finite group of linear transformations.* We shall usually employ the simpler expression *linear group.* The number of distinct transformations in the set (including the identity) is called the *order* of the group.

As an example of such a group take the four transformations consisting of the rotations of the $X-$, $Y-$ axes through 1, 2, 3, and 4 right angles around the origin in their plane:

$$A_1=\begin{bmatrix}0 & -1\\ 1 & 0\end{bmatrix},\quad A_2=\begin{bmatrix}-1 & 0\\ 0 & -1\end{bmatrix},\quad A_3=\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix},\quad E=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}. \tag{6}$$

For a second example, take the eight transformations consisting of the four rotations just given, in addition to these four accompanied by a reflexion on the new $Y-$ axis:

$$A_1,\ A_2,\ A_3,\ E;$$

$$B_1=\begin{bmatrix}0 & -1\\ -1 & 0\end{bmatrix},\quad B_2=\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix},\quad B_3=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix},\quad B_4=\begin{bmatrix}-1 & 0\\ 0 & 1\end{bmatrix}. \tag{7}$$

The former group is a *subgroup* of the latter.

The set of three transformations A_1, A_2, A_3 do not form a group, since the transformation A_2^2 (or $A_1 A_3$) is not found in the set.

Notation.—We shall reserve the letters G, H, K to denote particular groups that may come under discussion. The equation $G=(S_1, S_2, \ldots, S_g)$ implies that a given

group G consists of (or contains) the transformations S_1, S_2, . . . , S_g.

It is often convenient to use the phrase "(a group) G" with the same meaning as the phrase "the transformations of (a group) G." For instance, we may say "(something) is unaltered by G" instead of "(something) is unaltered by the transformations of G."

8. **Elementary properties of linear groups.—Generators.** Let G represent a given linear group, and S any transformation contained in G. Then it is easy to show that S is of finite order, say m, and that its different m powers (including its inverse and the identity) are contained in G. For, the series of transformations

$$S,\ SS=S^2,\ SS^2=S^3,\ \ldots$$

all belong to G and can evidently not form an unlimited number of distinct transformations, the group being finite. Hence, at least two of these powers are equivalent, say $S^a=S^{a+m}$, which may be written $S^aE=S^aS^m$. It follows that $E=S^m$ (§ 5). The transformation S is therefore of finite order (§ 6), and S^{m-1} is its inverse.

It may happen that the various powers of S exhaust the transformations of G. We then say that G is *generated* by S, and that S is a *generator* of G. If G contains other transformations, let T be one such, and the products S^aT^b, $S^aT^bS^c$, . . . all belong to G. We may be able to get all the transformations of G in this manner; if so, we say that S and T *generate* G, or that they form a *set of generators* of G; and so on.

Consider for example the group (6), § 7. Here $A_1^2=A_2$, $A_1^3=A_3$, $A_1^4=E$. Hence A_1 generates this group, which is also geometrically evident. In the case of (7) we have additional relations $A_1B_1=B_2$, $A_1^2B_1=B_3$, $A_1^3B_1=B_4$, so that A_1 and B_1 form a set of generators for this group.

Having given a linear group, a set of generators may usually be selected in different ways. It should be noted that a linear transformation selected at random will not generate a finite group (§ 6), and that two or more linear transformations each of finite order, but otherwise taken at random, will not generate a finite group.

9. **Collineations and collineation groups.** If $x_1, \ldots, x_n$ represent homogeneous co-ordinates in space of $n-1$ dimensions, then the geometrical effect of a linear transformation is not altered by multiplying all the elements in its matrix by an arbitrary constant. To illustrate, if x_1, x_2, x_3 represent trilinear co-ordinates of the plane, the transformations

$$A=\begin{bmatrix} 1 & 0 & 0 \\ -1 & 2 & -1 \\ 1 & -1 & 2 \end{bmatrix}, \qquad A'=\begin{bmatrix} 2 & 0 & 0 \\ -2 & 4 & -2 \\ 2 & -2 & 4 \end{bmatrix}$$

are both equivalent to the projective transformation leaving fixed the straight lines

$$x_1=0,\ x_2+x_3=0,\ x_1+x_2+x_3=0,\ x_1-x_2+x_3=0,$$

and transforming the point $(1,-2,\ 3)$ into the point $(1,\ 0,\ 1)$. We say that A and A' represent the same *collineation;* that is, a collineation is specified by the mutual ratios of the elements in the corresponding matrix, not by the actual values of these elements (to a given non-vanishing element may therefore at the outset be assigned at will any convenient number not zero). In practice it is customary to affix a factor of proportionality to either the old or the new variables to distinguish a collineation from a linear transformation; the collineation represented by the two transformations above will thus be written

$$\rho x_1=x_1',\ \rho x_2=-x_1'+2x_2'-x_3',\ \rho x_3=x_1'-x_2'+2x_3'.$$

The following laws obtain:

(*a*) If A and A' are linear transformations representing the same collineation, then there is a similarity-transformation S such that $A'=AS=SA$ (or $A'A^{-1}=A^{-1}A'=S$). Thus, in the example above, $S=(2, 2, 2)$. Conversely, S being any similarity-transformation, A and AS represent the same collineation.

(*b*) If A and A' represent the same collineation C_1, and similarly B and B' represent the same collineation C_2, then AB and $A'B'$ represent the same collineation C_1C_2.

For, let S and T be the two similarity-transformations $A'A^{-1}$ and $B'B^{-1}$, so that $A'=AS$, $B'=BT$, and we get $A'B'=ASBT=ABST$, since S is commutative with B (§ 6, Exercise 2). Hence, $(AB)^{-1}(A'B')=(AB)^{-1}(ABST)=(AB)^{-1}(AB)(ST)=ST$, which is a similarity-transformation (§ 4).

Hence, to find the product of two collineations, C_1 and C_2, we take the product of any two representative linear transformations. If therefore we have a finite set of collineations such that the product of any two of the set (whether alike or different) is a collineation of the set, we call this set a *collineation group* whose order is the number of distinct collineations of the set.

10. **The collineation group derived from a given linear group.** Let G be a linear group of order g, and A any one of its transformations. Furthermore, let $K=(S_1, S_2, \ldots, S_k)$ be the group consisting of all the similarity-transformations contained in G (§ 11, Exercise 1). Then (§ 9, (*a*))

$$AS_1,\ AS_2,\ \ldots,\ AS_k$$

are distinct linear transformations, all representing the same collineation, say C'. Moreover, no further transformations of G can represent C'.

If now B is a new transformation of G, we get a new collineation C'' corresponding to the transformations

$$BS_1, BS_2, \ldots, BS_k.$$

Proceeding thus, we shall finally arrange all the g transformations in g/k classes, giving rise to a set of g/k distinct collineations. These form a group of order g/k, since the product of any two of them belongs to the set (cf. § 9, (*b*)). We formulate this result as follows:

THEOREM 3. *To a given linear group G of order g corresponds a collineation group G' of order g/k, where k is the order of the group of similarity-transformations K contained in G. To a given collineation correspond k linear transformations of G, obtained from one of them by multiplying it in turn by each of the transformations of K.*

Example.—Let G be the group (6), § 7, of order 4. Here $K=(A_2, E)$, and we have two collineations in G', represented respectively by (A_2, E) and (A_1, A_3):

$$E': \rho x = x', \quad \rho y = y';$$
$$A_1': \rho x = -y', \quad \rho y = x'.$$

If a linear group G of order g contains no similarity-transformation other than the identity, then G will itself represent the corresponding collineation group. In other cases it may, or may not, contain a subgroup of linear transformations of order g/k which represents the collineation group corresponding to G. For instance, there is no linear group of order 2 contained in (6) whose collineation group is that one given in the example above. On the other hand, the group $E=(1, 1)$, $A_2=(-1, -1)$, $B_2=(1, -1)$, $B_4=(-1, 1)$ contains a subgroup which may be taken as its collineation group, namely E, B_2.

11. **Linear fractional groups.** A collineation in n variables $x_1, \ldots, x_n$ may be represented as a *linear fractional transformation* in the $n-1$ ratios $y_1=x_1/x_n, y_2=x_2/x_n, \ldots, y_{n-1}=x_{n-1}/x_n$. Assuming for simplicity $n=3$, the collineation corresponding to the linear transformation

$$x_1=a_{11}x_1'+a_{12}x_2'+a_{13}x_3', \quad x_2= \ldots, \quad x_3= \ldots,$$

as a transformation in the variable y_1, y_2, takes the form

$$y_1=\frac{a_{11}y_1'+a_{12}y_2'+a_{13}}{a_{31}y_1'+a_{32}y_2'+a_{33}}, \qquad y_2=\frac{a_{21}y_1'+a_{22}y_2'+a_{23}}{a_{31}y_1'+a_{32}y_2'+a_{33}}.$$

The transformations of K (cf. § 10) will all become the identity

$$y_1=y_1', \quad y_2=y_2',$$

and the k transformations representing a single collineation will give rise to a single linear fractional transformation. We thus obtain a *linear fractional group* of order g/k which is simply isomorphic (cf. § 32) with the collineation group G' and may be regarded as its equivalent.

Exercises

1. Prove that, in a linear group G, those transformations which have the canonical form make up a group by themselves. More particularly, the similarity-transformations make up a group K which is invariant under G (cf. § 31).

2. If G and G' are a linear group and its corresponding collineation group, then to the identity of G' correspond all the similarity-transformations of G.

3. From the formulas for the product of two linear transformations (§ 3) and the product of two determinants, prove that the product of the determinants of two transformations A and B is equal to the determinant of the transformation AB (cf. Exercise 1, § 6).

4. The determinant of the linear transformation A^m is the mth power of the determinant of A (cf. Exercise 3). Hence prove that the determinant of a transformation belonging to a linear group is a root of unity (cf. § 133). In particular, the determinant of a transformation of the third order is 1, ω or ω^2, where $\omega^3=1$.

5. Construct the collineation group corresponding to the group (7), § 7. Show that there is no subgroup of (7) of order 4 which may represent this collineation group.

12. **Groups of linear transformations of determinant unity.** The problem, having given a collineation group G' of order g' in n variables, to construct a corresponding linear group G, admits of an unlimited number of solutions (cf. § 9, (*a*)). We shall limit the problem by requiring the determinants of the linear transformations of G to be unity, and we shall show that under this condition the order of G is not greater than ng'.

Let A' be a linear transformation representing one of the collineations of G', and let its determinant be d. We then multiply it in turn by each of the n similarity-transformations $S_1, S_2, \ldots, S_n$, where

$$S_j = (r_j, r_j, \ldots, r_j),$$

$r_1, r_2, \ldots, r_n$ being the n different roots of the equation $r^n d = 1$. The n transformations so obtained all have a determinant $= 1$; moreover, no linear transformation outside these n will be of determinant unity and will represent the same collineation as A' (§ 9, (*a*)).

Taking each of the g' collineations in turn, we shall have constructed a table like that in § 10, containing ng' linear transformations in all. If A', B', C' are three collineations in G' such that $A'B' = C'$, then will the product of any transformation of our table from the line corresponding to A' and any transformation from the line corresponding to B', necessarily be a transformation from the line corresponding to C', since the determinant of this product is unity (Exercise 3, § 11). In other words, the ng' linear transformations form a linear group G, whose collineation group is G'.

Example.—Let $G' = (E, A)$, where $A = (1, -1)$. From E we obtain the two transformations E, $E_1 = (-1, -1)$; and from A the two $A_1 = (-i, i)$, $A_2 = (i, -i)$, where $i = \sqrt{-1}$. Therefore $G = (E, E_1, A_1, A_2)$.

It may happen that a group G_1 of transformations of determinant unity exists whose order is lower than ng' and whose collineation group is likewise G'. Its order must be divisible by g' and be a divisor of ng' (§§ 10, 28).

EXERCISES

1. Construct a group of order 3 of linear transformations of determinant unity whose collineation group is $(1, 1)$, $(1, \omega)$, $(1, \omega^2)$; $\omega^3 = 1$.

2. Construct the group of order 12 of transformations of determinant unity whose collineation group is

$$(1, 1), \begin{bmatrix} -1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ -1 & 1 \end{bmatrix}.$$

(As a linear fractional group, this group has the form

$$y=y',\ -y'+1,\ 1/y',\ 1/(-y'+1),\ 1-(1/y'),\ y'/(y'-1).)$$

13. **Change of variables.** For certain purposes it is of great convenience to introduce new variables which are linear functions of the old. To illustrate the theory let us consider the transformation (1), § 1:

$$S: \quad x = x' \cos\theta - y' \sin\theta, \quad y = x' \sin\theta + y' \cos\theta.$$

We shall now introduce new variables X, Y, where

$$(8) \qquad X = x + iy, \qquad Y = x - iy \qquad (i = \sqrt{-1}),$$

and correspondingly

$$(8') \qquad X' = x' + iy', \qquad Y' = x' - iy'.$$

The transformation S becomes

$$S': \qquad X = e^{i\theta} X', \qquad Y = e^{-i\theta} Y',$$

a result that can be expressed symbolically in terms of S and the change of variables (8), which we shall regard as a linear transformation.

Solving (8) for x, y we obtain

$$T: \qquad x=(X+Y)/2, \quad y=(X-Y)/2i.$$

Consider an arbitrary function $f(x, y)$. The transformation S changes f into the function

$$f(x' \cos\theta - y' \sin\theta,\ x' \sin\theta + y' \cos\theta),$$

which, expressed in terms of the variables X', Y', is the function

$$f\left(\frac{X'+Y'}{2}\cos\theta - \frac{X'-Y'}{2i}\sin\theta,\ \frac{X'+Y'}{2}\sin\theta + \frac{X'-Y'}{2i}\cos\theta\right).$$

On the other hand, we may at the outset express f as a function of the new variables: $f((X+Y)/2,\ (X-Y)/2i)$, and then transform it by means of S':

$$f\left(\frac{e^{i\theta}X'+e^{-i\theta}Y'}{2},\ \frac{e^{i\theta}X'-e^{-i\theta}Y'}{2i}\right).$$

Symbolically stated, the operator ST is equivalent to the operator TS':

$$(f)ST=(f)TS'.$$

Hence,

$$T^{-1}(ST)=T^{-1}(TS')=S'.$$

We formulate this result as follows for the general case:

THEOREM 4. *Having given a set of linear transformations A, B, . . . and a function f, involving n variables x_1, . . . , x_n, we may introduce new variables by means of a linear transformation*

$$T: \quad x_k=t_{k1}X_1+t_{k2}X_2+ \ . \ . \ +t_{kn}X_n \quad (k=1, 2, \ . \ . \ , n),$$

changing f into a function of X_1, . . . , X_n. As linear transformations in the new variables, A, B, . . . will take the forms $T^{-1}AT$, $T^{-1}BT$, . . .

We note that if $AB=C$, then $(T^{-1}AT)(T^{-1}BT) = T^{-1}CT$. Hence, if A, B, . . . form a group, so do $T^{-1}AT$, $T^{-1}BT$, . . . , and the two groups are simply isomorphic (§ 32).

14. **Transitive and intransitive groups.** Groups in two, three, and four variables whose transformations have respectively the following forms:

$$A=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix};\quad B=\begin{bmatrix} a & 0 & 0 \\ 0 & b & c \\ 0 & d & e \end{bmatrix};\quad C_1=\begin{bmatrix} p & q & 0 & 0 \\ r & s & 0 & 0 \\ 0 & 0 & t & u \\ 0 & 0 & v & w \end{bmatrix} \text{ or } C_2=\begin{bmatrix} p & 0 & 0 & 0 \\ 0 & a & b & c \\ 0 & d & e & f \\ 0 & g & h & j \end{bmatrix}$$

are said to be *intransitive.*

It may happen that a group can be made to assume the intransitive form by a suitable change of variables, though it does not possess this form initially. Consider, for example, a group G in four variables x_1, . . . , x_4 whose transformations are all of the following type:

$$\begin{bmatrix} a & b & e & f \\ b & a & f & e \\ h & g & c & d \\ g & h & d & c \end{bmatrix}.$$

The introduction of new variables y_1, y_2, z_1, z_2, where $y_1=x_1+x_2$, $y_2=x_3+x_4$; $z_1=x_1-x_2$, $z_2=x_3-x_4$, will change these matrices into the type C_1 above. That is, G has the intransitive form when written as a group in the variables y_1, y_2, z_1, z_2.

Definition. If the n variables of a group G can be separated into two or more sets (either directly or after a suitable change of variables), such that the variables of

any one set are transformed by all the transformations of G into linear functions of the variables of that set only, we say that G is *intransitive*. If such a division is not possible, the group is *transitive*. The different sets into which the variables of an intransitive group may be separated (as the sets (y_1, y_2) and (z_1, z_2) of the group above) are called its *sets of intransitivity*.

Exercises

1. Prove that a change of variables will not alter the form of a similarity-transformation.

2. Prove that $A'=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$ can be obtained from $A=\begin{bmatrix} a & 0 \\ c & b \end{bmatrix}$ by a suitable change of variables if $a \neq b$, and find the corresponding transformation T. (Hint: The condition $T^{-1}AT=A'$ gives $AT=TA'$. Multiply out and determine the elements in the matrix of T from the four resulting equations.)

3. Prove that if in type C_1, $t=p$, $u=q$, $v=r$ and $w=s$, then the two sets of intransitivity can be chosen in an infinite number of ways.

HERMITIAN INVARIANT AND REDUCIBILITY OF LINEAR GROUPS, §§ 15–20

15. **Conjugate-imaginary groups.** Let $G=(A, B, C, \ldots)$ be a linear group in the variables $x_1, \ldots, x_n$, and assume that the elements in the matrices of the various transformations are not all real. We may then separate the real and imaginary parts in both variables and coefficients; and by passing to the conjugate-imaginary values we evidently obtain a new group $\overline{G}=(\overline{A}, \overline{B}, \overline{C}, \ldots)$ in the variables $\bar{x}_1, \ldots, \bar{x}_n$ (we shall denote the conjugate-imaginary of a quantity w by $\overline{w}$), simply isomorphic with G (§ 32). For, if $AB=C$, it follows that $\overline{A}\,\overline{B}=\overline{C}$. We shall call either group *the conjugate-imaginary* of the other.

16. **Hermitian form.** The expression

$$J=\sum_{k=1}^{n}\sum_{l=1}^{n}q_{kl}x_k\bar{x}_l \qquad (q_{lk}=\bar{q}_{kl}),$$

subject to the condition that it vanishes only if $x_1=x_2=\ .\ .\ =x_n=0$, and is real and positive for all other sets of values that we may assign to these variables, is called a *positive-definite Hermitian form in the n variables* $x_1, \ .\ .\ .\ , x_n$, or simply *Hermitian form.* For instance, the expression $x_1\bar{x}_1+3x_2\bar{x}_2+(1+i)x_1\bar{x}_2+(1-i)x_2\bar{x}_1$ is a Hermitian form in the variables x_1, x_2.

THEOREM 5. *A positive-definite Hermitian form J in the variables $x_1, \ .\ .\ , x_n$ may be reduced to the form*

$$y_1\bar{y}_1+y_2\bar{y}_2+\ .\ .\ +y_n\bar{y}_n$$

by a change of variables of the following type:

$$y_1=p_{11}x_1, \quad y_2=p_{21}x_1+p_{22}x_2, \quad y_3=p_{31}x_1+p_{32}x_2+p_{33}x_3,$$
$$.\ .\ .\ .\ .$$
$$y_n=p_{n1}x_1+p_{n2}x_2+p_{n3}x_3+\ .\ .\ +p_{nn}x_n.$$

Proof.—Arranging J according to x_n and $\bar{x}_n$ we have

$$J=J_n=q_{nn}x_n\bar{x}_n+x_n\bar{X}_{n-1}+\bar{x}_nX_{n-1}+X,$$

where X_{n-1} represents a linear function of $x_{n-1}, \ .\ .\ , x_1$.

The coefficient q_{nn} is real and positive, since it is the value of J obtained by putting

$$x_n=1, \quad x_{n-1}=x_{n-2}=\ .\ .\ =x_1=0.$$

Accordingly, if we put

$$+\sqrt{q_{nn}}=+\sqrt{\bar{q}_{nn}}=p_{nn}, \text{ and } X_{n-1}=p_{nn}Y_{n-1},$$

we have

$$J_n=(p_{nn}x_n+Y_{n-1})(\bar{p}_{nn}\bar{x}_{n-1}+\bar{Y}_{n-1})+X-Y_{n-1}\bar{Y}_{n-1}$$
$$=y_n\bar{y}_n+J_{n-1},$$

where J_{n-1} is a Hermitian form in $n-1$ variables x_{n-1}, . . , x_1. For, it is of the required type and is the value of J_n obtained by subjecting the variables to the single condition $x_n = -Y_{n-1}/p_{nn}$. It is therefore real and positive unless $x_{n-1} = \ . \ . \ = x_1 = 0$.

We now arrange J_{n-1} according to x_{n-1} and $\bar{x}_{n-1}$, and proceed as above. We find

$$J_{n-1} = y_{n-1}\bar{y}_{n-1} + J_{n-2},$$

where y_{n-1} is a linear function of x_{n-1}, x_{n-2}, . . , x_1. Continuing thus, we finally prove the theorem.

17. **Lemma.** *If* $G = (T_1, T_2 \ . \ . \ . \ , T_g)$ *is a linear group, and* f *any function of the variables of the group, then the function*

$$I \equiv (f)T_1 + (f)T_2 + \ . \ . \ + (f)T_g \tag{9}$$

is either identically zero or is an "invariant" of G*; that is, it is transformed into itself by every transformation of* G.

Proof.—We have

$$\begin{aligned} (I)T_k &= (f)T_1T_k + (f)T_2T_k + \ . \ . \ + (f)T_gT_k \\ &= (f)T_1' + (f)T_2' + \ . \ . \ + (f_g')T_g', \text{ say}. \end{aligned} \tag{10}$$

But, T_1', T_2', . . , T_g' are the transformations T_1, T_2, . . , T_g over again in some order, since they all belong to G (§ 7) and are all distinct (§ 5; cf. Exercise 3, § 27). It follows that the last sum of (10) is equal to the right-hand member of (9); i.e., $I = (I)T_k$.

18. **Invariant Hermitian form.** We say that a Hermitian form J is *invariant under a group* G, or that J is a *Hermitian invariant* of G, when J is transformed into itself by the transformations of the intransitive group made up of G and its conjugate-imaginary group $\bar{G}$.

THEOREM 6. *There is always a Hermitian invariant J of a given linear group G in n variables.**

Proof.—Let the transformations of the group made up of G and $\bar{G}$ be denoted by $T_1, T_2, \ldots, T_g$, and let I represent the function $x_1\bar{x}_1+x_2\bar{x}_2+\ldots+x_n\bar{x}_n$. Then the function

$$J=(I)T_1+(I)T_2+\ldots+(I)T_g$$

is the required Hermitian invariant.

First, J is a Hermitian form in the variables $x_1, \ldots, x_n$. For every term $(I)T_k$ is the sum of n expressions $(x_s\bar{x}_s)T_k=X_s\bar{X}_s$, each of which is the product of two conjugate-imaginary quantities. The function J is therefore real and non-negative, and cannot vanish unless every term $(I)T_k$ vanishes. But if T_1 represents the identity, $(I)T_1=I$ and does not vanish unless every variable $x_1, \ldots, x_n$ vanishes. This is therefore also the case with J.

Second, J is transformed into itself by $T_1, \ldots, T_n$, by the lemma, § 17.

By aid of the theorems 5 and 6 we derive the

COROLLARY. *Such variables $x_1, \ldots, x_n$ may be selected for a linear group G that the function*

$$I=x_1\bar{x}_1+x_2\bar{x}_2+\ldots+x_n\bar{x}_n$$

is a Hermitian invariant of G.

19. **Unitary transformations.** A linear transformation $A=[a_{st}]$ whose coefficients satisfy the following relations:

$$(11)\quad a_{1k}\bar{a}_{1k}+a_{2k}\bar{a}_{2k}+\ldots+a_{nk}\bar{a}_{nk}=1 \qquad (k=1, 2, \ldots, n),$$

* This theorem was proved for $n=3$ by Picard and Valentiner (1887, 1889), and for any n by Fuchs, Loewy, and Moore (1896). See *Encyclopädie der mathematischen Wissenschaften*, Leipzig, 1898–1904, Bd. I, 1, p. 532.

$$(11') \quad a_{1k}\bar{a}_{1l}+a_{2k}\bar{a}_{2l}+ \ . \ . \ +a_{nk}\bar{a}_{nl}=0 \qquad (k, l=1, 2, \ . \ . \ , n; \ k\neq l),$$

$$(12) \quad a_{k1}\bar{a}_{k1}+a_{k2}\bar{a}_{k2}+ \ . \ . \ +a_{kn}\bar{a}_{kn}=1 \qquad (k=1, 2, \ . \ . \ , n),$$

$$(12') \quad a_{k1}\bar{a}_{l1}+a_{k2}\bar{a}_{l2}+ \ . \ . \ +a_{kn}\bar{a}_{ln}=0 \qquad (k, l=1, 2, \ . \ . \ , n; \ k\neq l),$$

is said to have the *unitary form.*

The variables of a group being selected so that its Hermitian invariant is $x_1\bar{x}_1+ \ . \ . \ +x_n\bar{x}_n$, we readily find that the corollary of § 18 is tantamount to the following statement: *such variables may be selected for a linear group that its transformations all have the unitary form.*

The equations (11), (11′) are deduced directly; and the equations (12), (12′) by operating on the Hermitian form by A^{-1}, as given below.

The inverse of a transformation in unitary form can be written down at once:

$$A^{-1}: \ x_k=\bar{a}_{1k}x_1'+\bar{a}_{2k}x_2'+ \ . \ . \ +\bar{a}_{nk}x_n' \quad (k=1, 2, \ . \ . \ , n).$$

For, the condition $A^{-1}A=(1, 1, \ . \ . \ , 1)$ leads to the equations (11), (11′).

20. **Reducible and irreducible groups.** A linear group in n variables is said to be *reducible* when, after a suitable choice of variables $x_1, \ . \ . \ , x_n$, a certain number of these (say $x_1, x_2, \ . \ . \ , x_m; \ m<n$) are transformed into linear functions of themselves by the transformations of the group. (Thus, a group in three variables x_1, x_2, x_3, whose matrices have the form

$$\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & g \end{bmatrix}$$

is reducible.) We shall say that the m variables $x_1, \ldots, x_m$ constitute *a reduced set* of the group.

An *irreducible* group is a group in which no such choice of variables is possible.

THEOREM 7. *A reducible group G is intransitive, and a reduced set becomes a set of intransitivity.*

Applied to the reducible group in three variables indicated above, the theorem asserts that new variables may be introduced such that the matrices are of type B, § 14, and that the original variables x_1, x_2 will form a set of intransitivity of the new.

Proof.—A Hermitian invariant of G may be reduced to the form $y_1\bar{y}_1 + \ldots + y_n\bar{y}_n$ by the change of variables specified in § 16. The group G will still have the typical form of a reducible group, whose matrices we shall write symbolically

$$\begin{bmatrix} A' & 0 \\ A'' & A''' \end{bmatrix},$$

and it remains for us to prove that the elements in A'' are all zero.

For this purpose we write down as many of the equations (12) and as many of the equations (11) as contain elements of A'''; namely the last $n-m$ in each case. If we then subtract the sum of the latter equations from the sum of the former, there results an equation $\Sigma a_{st}\bar{a}_{st} = 0$, in which the left-hand member contains one term for each of the elements of A''. Now, each of these terms is real and non-negative; consequently the sum $\Sigma a_{st}\bar{a}_{st}$ cannot vanish unless every number $a_{st} = 0$. That is, the elements of A'' are all zero, and the theorem is proved.

The validity of the proof is evidently not impaired by assuming the given reducible group G to be a subgroup of a larger group H, reducible or irreducible. Furthermore, the final *intransitive* group G is composed of unitary

transformations, by the process of proof; and this result is equally true of H (let the initial Hermitian invariant used in the proof be the Hermitian invariant of H). Thus, with slight modifications of the above proof as to detail, which will be left as an exercise for the student, we obtain the following important

THEOREM 8. *Having given a linear group H containing an intransitive subgroup G, we may choose such variables that G appears in intransitive form* (cf. types A–C, § 14), *and that at the same time the transformations of H are all unitary.*

EXERCISES

1. Show that a unitary transformation in two variables and of determinant unity has the form

$$\begin{bmatrix} p & q \\ -\bar{q} & \bar{p} \end{bmatrix}; \qquad p\bar{p}+q\bar{q}=1 .$$

2. Prove by the method of § 18 that if all the elements in the matrices of G are real, then there is a quadratic function of the variables which is invariant under G.

3. Find the most general type of a Hermitian invariant of a linear group which contains a transformation in canonical form whose multipliers are all distinct, as $(1, \omega, \omega^2)$; $\omega^3=1$.

4. Prove that if a group G possesses a Hermitian invariant which does not contain all the variables of G, then this group is intransitive.

5. If there exists a linear function of the variables of a group G which is invariant under G, then this group is intransitive.

In the case of a substitution group (chap. ii) written as a linear group (§ 1) there is such a function, namely the sum of the letters of substitution. Hence this group is always intransitive.

CANONICAL FORM OF A LINEAR TRANSFORMATION AND OF ABELIAN GROUPS, §§ 21–22

21. Theorem 9. *A linear transformation of finite order will assume the canonical form by a suitable choice of variables.*

Proof.—Let the transformation be $A=[a_{st}]$. We can determine a linear function which is transformed into a certain constant multiple of itself by A, say $(y_1)A=\theta y_1$, where $y_1=b_1x_1+\ .\ .\ .\ +b_nx_n$. To obtain the necessary conditions we equate the coefficients of the variables $x_1, \ .\ .\ .\ , x_n$, and find the equations

$$b_1a_{1t}+b_2a_{2t}+\ .\ .\ .\ +b_na_{nt}=\theta b_t \qquad (t=1, 2, \ .\ .\ .\ , n),$$

which can be solved for $b_1, \ .\ .\ .\ , b_n$ provided θ is a root of the *characteristic equation* of A (cf. § 23).

Having thus determined y_1 we change to new variables such that y_1 is one of these. The group generated (§ 8) by A is now seen to be reducible, since

$$(y_1)A=\theta y_1, \ (y_1)A^2=\theta^2 y_1, \text{ etc.},$$

from which it follows that the first row in the matrices of each of these transformations is of the form

$$k \ 0 \ 0 \ .\ .\ 0,$$

where k represents different powers of θ in the different transformations. Hence, by Theorem 7, § 20, the group in question is intransitive, and y_1 constitutes one of its sets of intransitivity. Let $(y_2, \ .\ .\ .\ , y_n)$ be the other (temporary) set of intransitivity.

The foregoing process may now be repeated for the set $(y_2, \ .\ .\ .\ , y_n)$ in place of the original n variables. A new linear function will be determined which is transformed into a constant multiple of itself by A, and the set $(y_2, \ .\ .\ .\ , y_n)$ will break up into further sets of intransitivity. Continuing thus, we finally obtain A in the desired canonical form.

22. **Canonical form of abelian group.** The group consisting of the different powers of a transformation A

is an example of a type of group called *abelian;* namely a group in which all the operators are commutative (§ 4); i.e., if A and B are two operators of the group, then $AB=BA$.

THEOREM 10. *In any given abelian group K of linear transformations, such new variables may be introduced that all the transformations of K will simultaneously have the canonical form.*

Proof.—If the group contains only similarity-transformations (§ 2) the theorem is self-evident. Hence we assume in K a transformation S which is not a similarity-transformation. Let the variables of the group be chosen such that S appears in the canonical form (§ 21):

$$S=(\alpha, \ . \ . \ , \lambda).$$

The multipliers of S may not all be distinct. Suppose that m of them are equal (say to α), and differ in value from all the others; we shall then show that K transforms the corresponding variables into linear functions of themselves and is therefore intransitive (§ 20).

Let f be any linear function of the m variables in question, say $x_1, x_2, \ . \ . \ , x_m$. We have $(f)S=\alpha f$; moreover, any linear function F such that $(F)S=\alpha F$ can evidently not contain any of the variables $x_{m+1}, \ . \ . \ , x_n$.

Let now T be any transformation of K. We have $ST=TS$, and if we put $(f)T\equiv f'$ we get

$$(f)TS=(f')S=(f)ST=\alpha f'.$$

That is, the function f', which is linear in the variables of the group, must be a function of $x_1, \ . \ . \ , x_m$ only, by what has just been said. It follows that K is intransitive.

If we now confine our attention to one of its sets of intransitivity, we may apply anew the process above to that set. This will, therefore, break up into further sets of intransitivity. Continuing thus, the ultimate sets of intransitivity will contain one variable each, and the theorem is proved.

We shall often say: "let a (given) transformation (or group) be written in canonical form" instead of "let the variables be so chosen that a (given) transformation (or group) will appear in the canonical form."

From the theorems 8 and 10 we deduce the

COROLLARY. *Such variables may be selected for the variables of a linear group G that a given abelian subgroup of G is written in the canonical form, and that at the same time the transformations of G are all unitary.*

23. Characteristic and characteristic equation. If we add $-\theta$ to each of the elements in the principal diagonal of the matrix of a linear transformation $A=[a_{st}]$ and equate to zero the resulting determinant, we have an equation in θ which is called the *characteristic equation of A:*

$$\begin{vmatrix} a_{11}-\theta & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22}-\theta & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1} & a_{n2} & \cdots & a_{nn}-\theta \end{vmatrix} = 0 . \tag{13}$$

THEOREM 11. *If T and A are linear transformations, the roots of the characteristic equation of A are the same as those of $T^{-1}AT$.*

Proof.—Put $T^{-1}AT=B=[b_{st}]$, whose characteristic equation is

$$\begin{vmatrix} b_{11}-\theta & \cdots & b_{1n} \\ \cdots & \cdots & \cdots \\ b_{n1} & \cdots & b_{nn}-\theta \end{vmatrix} = 0 . \tag{14}$$

Regarding θ as a variable temporarily, we shall look upon the left-hand members of (13) and (14) as the matrices of linear transformations which we shall write symbolically $(A-S)$ and $(B-S)$, where S represents the similarity-transformation $(\theta, \ldots, \theta)$. Then, since $T^{-1}AT=B$ and $T^{-1}ST=S$, we readily find that $T^{-1}(A-S)T=(B-S)$. Hence, if the determinants of T, $(A-S)$ and $(B-S)$ are denoted by t, a, and b respectively, we have (cf. Exercise 3, § 11) $t^{-1}at=b$, giving $a=b$. Accordingly, the coefficients of the various powers of θ in a and b are equal, and the theorem follows.

The sum of the characteristic roots of A is called the *characteristic* of A. It is equal to the sum of the elements in the principal diagonal of A, namely $a_{11}+a_{22}+\ldots+a_{nn}$.

Exercises

1. Find the characteristic roots of a transformation written in canonical form.

2. Prove that the characteristic roots of a linear transformation of finite order are roots of unity (cf. §§ 4, 6, 21, 23, 133).

3. Can the variables be so changed that $S=\begin{bmatrix} 1 & 0 \\ -1 & 1 \end{bmatrix}$ will assume the canonical form?

CHAPTER II

GROUPS OF OPERATORS AND SUBSTITUTION GROUPS

A. Groups of Operators

24. **Introduction.** The notion of a group was introduced in § 7. While this term has been associated hitherto with linear transformations only, there are so many important properties of groups of operators which are independent of their mode of representation, that it seems best to study such properties apart from the form that these groups take. The usefulness of the results derived will in this way not be limited to the realm of linear groups.

In addition we need a certain amount of knowledge of substitution groups for the development of linear groups. However, beyond a general introduction to the theory of groups of operators and substitution groups, only such additional theorems in either field as are needed for this development will be given here. For a detailed account in the English language of abstract and substitution groups, the reader may with profit consult the following books:

E. Netto, *The Theory of Substitutions and Its Applications to Algebra* (tr. by F. N. Cole). Ann Arbor, Mich.: Inland Press, 1892.

W. Burnside, *Theory of Groups of Finite Order.* 2d ed. Cambridge University Press, 1911.

H. Hilton, *An Introduction to the Theory of Groups of Finite Order.* Oxford, 1908.

G. A. Miller, H. F. Blichfeldt, and L. E. Dickson, *Theory and Applications of Finite Groups.* New York: John Wiley & Sons, 1916.

OPERATORS AND GROUPS OF OPERATORS, §§ 25–28

25. **Operators.*** We postulate a certain class O of objects called operators having the following properties:

1°. If A and B are any two operators, then either A and B are *equal* $(A=B)$ or *distinct* $(A\neq B)$.

That is, the operators are so defined that it shall be possible for us in any case to determine whether two given operators are equal or not. Thus, if O is the class of all linear transformations in two variables, two operators A and B, defined by their matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \text{ and } \begin{bmatrix} p & q \\ r & s \end{bmatrix},$$

are equal when the following (ordinary) equations are satisfied: $a=p$, $b=q$, $c=r$, $d=s$; if O is the class of all collineations in two variables, the two corresponding operators are equal if a number k can be found such that the equations $a=pk$, $b=qk$, $c=rk$, $d=sk$ are satisfied.

2°. Whether $A=B$ or $A\neq B$, there is a unique operator C called the *product* of A and B; in symbols $AB=C$.

Here we assume that a certain rule for forming the product AB (cf. § 3) is given, producing an operator C in O, which is "unique" in the sense that if more than one operator results from the rule, then any two such operators are equal (cf. § 9).

3°. The *associative law* holds for a product of three operators: $(AB)C=A(BC)$; that is, if $AB=S$, $BC=T$, then $SC=AT$.

4°. There is a unique operator E called *the identity* and having the property that, for every operator A, we have $AE=A$ and $EA=A$.

5°. The operators are reversible in O; that is, to every operator A there corresponds a unique operator in O

* The development of chap. i is followed closely in §§ 25–27. For a bibliography and discussion of various definitions of abstract groups consult E. V. Huntington, *Transactions of the American Mathematical Society*, VI (1905), 181 ff. The postulates 4° and 5° above demand more than is logically necessary (cf. L. E. Dickson, *Transactions of the American Mathematical Society*, *ibid.*, p. 199).

called the *inverse* of A and denoted by A^{-1}, such that we have $AA^{-1}=E$.

In 4° and 5° the word "unique" is interpreted as in 2°.

6°. The following relations of equality obtain, as in the case of ordinary (numerical) equality: (*a*) $A=A$; (*b*) if $A=B$, then $B=A$; (*c*) if $A=B$ and $B=C$, then $A=C$; (*d*) if $A=B$ and $C=D$, then $AC=BD$.

Remark.—Our conception of the class of operators O involves necessarily another class F, composed of *subjects of operation*. To give some illustrations: (*a*) let F represent all polynomials in n variables and O all linear transformations in those variables; (*b*) let F represent all points in the plane and O all rotations in that plane around a given point, accompanied or not by inversions with respect to the given point; (*c*) let F represent n points on a line and O the different permutations of those points. However, in the present chapter the class F is practically never referred to.

The product AB is not necessarily the same as the product BA. If the two products are equal ($AB=BA$), we say that the operators A and B are *commutative*. A continued product of any number of operators A, B, C, D, . . may be obtained by taking the product of two of them (say AB), then the product of this product and an operator, etc., giving say $(((AB)C)D)$ . . . . By 3° it follows that the factors in the final product may be reassociated in any manner (as $(AB)(CD)$ . .), so long as their order in the product is not disturbed.

In the future we shall often say "a (set, group, class) G contains an operator S," "S is found among the operators of G," "S is an operator of G," or simply "S belongs to G," instead of "S is equal to one of the operators of G."

EXERCISES

1. Prove that the inverse of the identity is the identity (i.e., $E^{-1}=E$), and that the inverse of A^{-1} is A (i.e., $A^{-1}A=E$).

(Hint: let A' be the inverse of A^{-1}, then $A^{-1}A'=E$. Now apply 3° to the left-hand member of $A(A^{-1}A')=AE$.)

2. Prove that, if $AB=AC$, or if $BA=CA$, then $B=C$.

3. Prove that $(S^{-1}AS)(S^{-1}BS)=S^{-1}(AB)S$.

4. Let the operators $A_1, A_2, \ldots$ of a class O be represented by the symbols $(x_1, y_1), (x_2, y_2), \ldots$, under the condition that two operators are equal $(A_1=A_2)$ only if the two equations $x_1=x_2$, $y_1=y_2$ are satisfied. Now if the product A_1A_2 is expressed by the formula

$$(x_1, y_1)(x_2, y_2)=(x', y'),$$

where $x'=x_1x_2-y_1y_2$, $y'=x_1y_2+y_1x_2$, prove that the conditions $1^\circ-6^\circ$ are fulfilled, and find the identity and the inverse of A_1. (To give an example of an operator of this type: let operating by A_1 consist in multiplying by the complex number $x_1+\sqrt{-1}y_1$.)

If the product is $(x', y')=(x_1x_2, x_1y_2)$, prove that 1°, 2°, 3°, 6° are fulfilled.

5. Prove that the inverse of the operator AB is $B^{-1}A^{-1}$.

26. **Power and order of an operator.** As in § 4, we write A^2 for AA, A^3 for $A(A^2)$ or $(A^2)A$, $\ldots$, A^m for $A(A^{m-1})$ or $(A^{m-1})A$, and call these products the 2d, 3d, $\ldots$, mth *powers* of A. We also write A^{-m} for $(A^m)^{-1}$, and if we put $A^0=E$ we have

$$A^nA^m=A^{n+m}, \quad (A^n)^m=A^{nm}, \quad E^n=E,$$

where m and n are positive or negative integers or zero.

If a certain power of the operator A equals the identity, then A is of *finite order;* and the least positive integer m such that $A^m=E$ is called the *order* of A. We shall prove the following propositions:

(*a*) If $A^n=E$, then n is a multiple of m. For if not, let r be the remainder when n is divided by m, so that $n=mq+r$, and $r<m$. Then $A^n=A^{mq+r}=A^{mq}A^r=E^qA^r=A^r=E$, which is contrary to the hypothesis that A^m is the least power of A which equals E.

(*b*) The order of A^k is m/d, where d is the highest common factor of m and k. For, the order of A^k is the least positive integer t for which $E=(A^k)^t=A^{kt}$; i.e., for which kt is a multiple of m, by (*a*). Hence, $kt/m=$ an integer; and

canceling the common factor d from k and m, the remaining factor of m (namely m/d) must divide t; that is, $t=m/d$.

27. **Finite groups. Generators.** We shall now take up the study of sets of operators called *finite groups.*

DEFINITION. *A set of g distinct operators $S_1, S_2, \ldots, S_g$ in* O *form a group G of order g if the product of any two of them, whether equal or distinct, is an operator of the set.* We write $G=(S_1, S_2, \ldots, S_g)$.

If $H=(T_1, T_2, \ldots, T_g)$ is another group containing the same operators as G, we write $G=H$. We are, however, not to infer that the operators are arranged in the same order; that is, $G=H$ does not necessarily imply $S_1=T_1, \ldots, S_g=T_g$. If there is at least one operator in G not found in H, or vice versa, we shall say that the two groups are distinct ($G\neq H$).

Example 1.—Let O consist of all rotations of a sphere around its center. The three rotations, each of 180°, around each of three mutually perpendicular diameters, together with the identity (no rotation), form a group of order 4.

Example 2.—Let O consist of the different permutations of four points a, b, c, d on a line. The four permutations (§ 40):

$$\begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix}, \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}$$

form a group of order 4.

We find, as in § 8, that the identity belongs to G; that each operator of G is of finite order; and that the inverse of each operator of G is an operator of G.

We shall, obviously, exclude from the concept "group" the (trivial) group consisting of the single operator E.

GENERATORS. A set of operators $A, B, \ldots$ of G having the property that every operator S of G is expressible as a product of the operators of the set: $S=\ldots A^aB^b \ldots A^cB^d \ldots$, is called a *set of generators*

of G. Thus, any two of the rotations of 180° in the group of Example 1 above will generate that group.

EXERCISES

1. Prove that a set of operators will form a group H if it be known that they belong to a given group and that the product of any two of them, alike or distinct, is an operator of the set H.

2. Show that if A, B, . . . belong to a group G, then any product of three or more of these operators, as for instance $A^{-1}BA$, is again an operator of G.

3. Let S_1, S_2, . . . , S_g be the different operators of a group G, and let S represent any one of them. Prove that the g operators obtained by taking the products S_1S, S_2S, . . . , S_gS are all distinct and are therefore the operators of G over again in some order.

4. Find a set of two generators of the group in Example 2 above.

5. Consider the symbols (x_1, y_1), . . . of Exercise 4, § 25, the rule for a product being the first of the two there given. Prove that (0, 1) is a generator of a group of order 4. Prove also that the two symbols $(-1, 0)$, $(-1/2, \sqrt{3}/2)$ generate a group of order 6.

Both of these groups are abelian (§ 34).

6. Prove that the operators common to two groups form by themselves a group.

28. **Subgroups.** A group H of order h, all of whose operators are found among those of a group G, is called a *subgroup* of G. Strictly speaking, H is not thought of as a subgroup unless $h<g$, but we shall here generally understand the definition in such a way that G is a subgroup of itself $(h=g)$.

THEOREM 1. *The order of a group G is divisible by the order of a subgroup H of G:* $g=hk$. The quotient $g/h=k$ is called the *index* of H.

The proof is based on our arranging the operators of G in the form of a rectangle of h columns and k rows:

$$
\begin{array}{ll}
 & E,\ S_2,\ \ldots,\ S_h; \\
 & V_2,\ S_2V_2,\ \ldots,\ S_hV_2; \\
(1) & V_3,\ S_2V_3,\ \ldots,\ S_hV_3; \\
 & \cdots\cdots\cdots\cdots \\
 & V_k,\ S_2V_k,\ \ldots,\ S_hV_k.
\end{array}
$$

The first row is composed of the operators of H; V_2 is an operator of G not found among those of the first row; V_3 is an operator of G not found among those of the first two rows, etc. New rows are added in this manner until every operator of G has been accounted for. It remains for us to prove that the hk operators obtained are all distinct.

First, the operators in any one row are distinct. For the assumption $S_aV_c=S_bV_c$ gives $S_a=S_b$ (Exercise 2, § 25), which is contrary to the hypothesis that the first row is composed of the distinct operators of H.

Second, the operators from two different rows are distinct. For if, say, $S_aV_c=S_bV_d$, $c<d$, we should have $S_b^{-1}(S_aV_c)=S_b^{-1}S_bV_d$; that is, $V_d=S'V_c$, where $S'=S_b^{-1}S_a$ and therefore belongs to H, since S_b^{-1} and S_a do that. But then V_d would occur in a previous row (the cth), contrary to hypothesis.

It follows that the table contains all the operators of G, once each. The theorem is therefore proved.

We shall indicate the rows symbolically by H, HV_2, . . . , HV_k, and write

$$G=H+HV_2+\ .\ .\ +HV_k.$$

It is to be noticed that the h operators in any one row, except the first, do not form a group.

COROLLARY. *The order of an operator S of a group G is a factor of the order g.* For, if m is the order of S, the m operators E, S, S^2, . . . , S^{m-1} form a subgroup of G.

Remark.—Though the order of a subgroup of G is a factor of the order of G, it is not true in general that there is a subgroup whose order is any given factor of g, unless this factor is a power of a prime number (cf. § 36, and Exercise 1, § 38).

EXERCISES

1. Find the subgroups of order 2 of the group in Example 1, § 27.

2. Construct a subgroup of order 2 and one of order 3 of the collineation group given in Exercise 2, § 12.

CONJUGATE SETS, §§ 29–31

29. Having defined groups and subgroups, we now introduce the first of two important concepts, **conjugate sets** and **isomorphism.**

DEFINITION. If A and S are operators belonging to a group, then A and $S^{-1}AS$ are said to be *conjugate.* We also say that the first of these operators is *transformed into* the last by S.

The following propositions (a) and (b) are easily verified by the student:

(a) *There is an operator which transforms* $S^{-1}AS$ *into* A, *namely* S^{-1}. It follows that the relationship expressed by "conjugate" is reciprocal.

(b) *If* A *and* B *are conjugate, and also* B *and* C, *then* A *and* C *are conjugate.* (Prove that if A is transformed into B by S ($B=S^{-1}AS$), and B into C by T, then A is transformed into C by ST: $C=(ST)^{-1}A(ST)$.)

Now let S be any one of the operators of the group $G=(E, S_2, \ldots, S_g)$. Consider the conjugates:

$$E^{-1}SE=S,\ S_2^{-1}SS_2,\ \ldots,\ S_g^{-1}SS_g. \tag{2}$$

They are not all distinct: all the operators $E, S, \ldots$ of G which are commutative with S (and only those) transform S into itself. For, from $S=S_a^{-1}SS_a$ follows $S_aS=SS_a$ and vice versa. We therefore select a representative of each distinct conjugate and get what is called a *complete set* (or simply *set*) *of conjugate operators under* G.

(c) *A conjugate set* $A, B, \ldots$ *is transformed into itself by any operator* S' *of* G. For, if $A=S_a^{-1}SS_a$, $B=S_b^{-1}SS_b, \ldots$ are distinct conjugates, so are $S'^{-1}AS'$, $S'^{-1}BS', \ldots$, and if the former set is taken from the series (2), the latter must belong to (2) also, since $S'^{-1}(S_a^{-1}SS_a)S'=(S_aS')^{-1}S(S_aS')$, etc. (cf. Exercise 5, § 25).

The number of operators in a conjugate set is determined by the following:

THEOREM 2. *All the operators E, S_a, S_b, . . . of G which are commutative with S form a subgroup H of G, say of order h, and the conjugate set of G to which S belongs contains g/h distinct operators.*

To prove the first statement, we need merely to show that the operator S_aS_b is commutative with S (Exercise 1, § 27). This is done as follows:

$$(S_aS_b)S = S_a(S_bS) = S_a(SS_b) = (S_aS)S_b = (SS_a)S_b = S(S_aS_b) .$$

To prove the second, consider the table (1), § 28. The operators in the first line will all transform S into itself, since they are here commutative with S. All those in the second line will transform S into one and the same (new) operator $V_2^{-1}SV_2$. For, S_aV_2 being any operator of HV_2, we have

$$(S_aV_2)^{-1}S(S_aV_2) = V_2^{-1}(S_a^{-1}SS_a)V_2 = V_2^{-1}SV_2.$$

Moreover, $V_2^{-1}SV_2$ is distinct from S, as otherwise V_2 would be commutative with S and would therefore belong to H. Similarly, the operators of the third line all transform S into a third operator $V_3^{-1}SV_3$, distinct from S and from $V_2^{-1}SV_2$. Thus, suppose $V_3^{-1}SV_3 = V_2^{-1}SV_2$; then S would be commutative with $V_3V_2^{-1}$, so that this operator would be an operator in H, say S_a. Hence $V_3 = S_aV_2$. But this is impossible, since V_3 is not found among the first two lines of the table (1). Proceeding thus, we obtain a distinct conjugate for each line of the table, and the theorem is proved.

30. **Conjugate subgroups.** If we transform the operators E, S_2, . . . , S_k of a subgroup K of G by an operator of G, say V, we obtain the same or another subgroup

which we shall designate $V^{-1}KV$. For, the resulting k operators belong to G, and the product of any two of them:

$$(V^{-1}S_aV)(V^{-1}S_bV) = V^{-1}S_aVV^{-1}S_bV = V^{-1}(S_aS_b)V,$$

is contained in the set $V^{-1}KV$, since S_aS_b is an operator of K.

We say that K and $V^{-1}KV$ are *conjugate subgroups* of G. If the two groups are equal ($K = V^{-1}KV$; cf. § 27), we say that V is *commutative* with K.

The reader may verify the propositions corresponding to (*a*), (*b*), and (*c*), § 29, namely that $V^{-1}KV$ is transformed into K by V^{-1}, that two groups conjugate to a third are conjugate to each other, and that a set of conjugate subgroups of G is transformed into the same set by an operator of G. Finally, the following theorem may be proved in the same manner as the corresponding theorem above:

THEOREM 2′. *All the operators of G which are commutative with K* (among these are found the operators of K) *form a subgroup H' of order h', and the number of distinct subgroups of G conjugate to K is g/h'.*

EXERCISES

1. Prove that the operators AB and BA are conjugate.

2. Prove that conjugate operators, or conjugate subgroups, have the same order.

3. If two commutative operators, A and B, are transformed by an operator S, the new operators are also commutative.

Hence, the conjugate of an abelian group (§ 34) is again an abelian group.

4. If H is the group whose operators are commutative with S (cf. Theorem 2), then $T^{-1}HT$ is the group whose operators are commutative with $T^{-1}ST$.

5. Prove that two sets of conjugate operators have either no operators in common or are composed of the same operators.

Hence show that the operators of G can be separated into distinct conjugate sets, the total number of whose operators is equal to the

order (g) of the group. At least one set contains only one operator, namely the identity. Accordingly, if these sets contain respectively 1, k_2, k_3, . . operators, we have $g=1+k_2+k_3+ \ . \ . \ .$ Furthermore, we have (Theorem 2) $k_2=g/h_2$, $k_3=g/h_3$, . . , so that finally

$$1=\frac{1}{g}+\frac{1}{h_2}+\frac{1}{h_3}+ \ . \ .$$

31. **Invariant operators and subgroups. Simple groups.** We say that the operator S is *invariant under* G, or that it is a *self-conjugate* operator of G, when S is transformed into itself by every operator of G (that is, if the operators (2), § 29, are all equal).

Similarly, we say that a subgroup H of G is *invariant under* G or is a *self-conjugate* subgroup of G, when $H=S_2^{-1}HS_2= \ . \ . \ =S_g^{-1}HS_g$.

Thus, the operator S is invariant under H in Theorem 2, and the group K is invariant under H' in Theorem 2′. Any group is an invariant subgroup of itself (§ 28).

A group which contains no invariant subgroups (except itself) is called a *simple* group.

EXERCISES

1. If G is a simple group, none of the numbers k_2, k_3, . . of Exercise 5, § 30, can be unity.

2. Prove that a group of order 5 is simple.

More generally, a group whose order is a prime number is simple. The least composite number which can be the order of a simple group is 60 (§ 48).

3. The operators of a conjugate set of a group G generate an invariant subgroup of G.

(Observe that the operators of a group G' generated by A, B, C, . . are of the form

$$T= \ . \ . \ . \ A^pB^qC^r \ . \ . \ A^sB^tC^v \ . \ . \ .$$

The condition that G' be transformed into itself by an operator S of G is that $S^{-1}TS$ belongs to G'. Now, if $S^{-1}AS$, $S^{-1}BS$, . . are denoted by A_1, B_1, . . , we have (Exercise 3, § 25):

$$S^{-1}TS= \ . \ . \ . \ A_1^pB_1^qC_1^r \ . \ . \ A_1^sB_1^tC_1^v \ . \ . \ .$$

In other words, if G' is generated by $A, B, C, \ldots$, then $S^{-1}G'S$ is generated by $A_1, B_1, C_1, \ldots$ But, these last operators belong to the conjugate set in question if $A, B, C, \ldots$ do that (§ 29), (c).)

4. Prove that any two invariant operators of G are commutative, and that their product is also an invariant operator of G.

Hence prove that all the invariant operators of G form an abelian group H (§ 34) which is invariant under G. Furthermore, any subgroup of H is an invariant subgroup of G.

5. Show that a similarity-transformation belonging to a linear group G is invariant under G, and that the group of similarity-transformations contained in G is an invariant subgroup of G.

6. Prove that the transformations of determinant unity contained in a linear group G is a self-conjugate subgroup of G.

ISOMORPHISM, §§ 32–33

32. It is sufficiently evident from the preceding development that the theory of groups of operators depends entirely upon the scheme according to which the products of operators are tabulated (the "multiplication table" of the group.)* Two groups whose multiplication tables are the same have essentially the same abstract properties, differing only in the notation and possibly the meaning of their operators. The relationship is expressed in the following:

DEFINITION. Two groups, G and K, are said to be *simply isomorphic* when their distinct operators are equal in number and can be arranged in relative order such as:

$$G: E, S_2, S_3, \ldots, S_g;$$
$$K: E, T_2, T_3, \ldots, T_g,$$

so that their products all correspond; that is, if $S_aS_b = S_c$, then $T_aT_b = T_c$.

Example 1.—The groups of order 4 in Examples 1 and 2, § 27, are simply isomorphic.

* It will be seen later (§ 47) that if a multiplication table is arbitrarily constructed, so that only the conditions of §§ 25 and 27 are complied with, then there is at least one group of operators (a substitution group) whose multiplication table is the one given.

On the other hand, these groups are not isomorphic with the group $G=(E, S_2, S_3, S_4)$ whose operations consist in multiplying by $1, i, -1, -i$ respectively, where $i=\sqrt{-1}$. The square of every operator of the first two groups is the identity; but this is not the case with S_2 or S_4 of the present group.

Example 2.—Two conjugate groups, $H=(E, A, B, \ldots)$ and $V^{-1}HV=(E, V^{-1}AV, V^{-1}BV, \ldots)$, are simply isomorphic.

A more general kind of isomorphism may sometimes be established between two groups, K of order k and G of order $g=kh$. For instance, let it be possible to arrange their operators in the following manner:

$$
\begin{array}{lll}
 & K: & G: \\
 & T_1=E; & S_{11}, S_{12}, \ldots, S_{1h}; \\
(3) & T_2; & S_{21}, S_{22}, \ldots, S_{2h}; \\
 & \cdot & \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\
 & T_k; & S_{k1}, S_{k2}, \ldots, S_{kh};
\end{array}
$$

so that first, to each operator of K there correspond h operators of G; and second, to each product $S_{a\alpha}S_{b\beta}=S_{c\gamma}$ there corresponds a product $T_aT_b=T_c$, irrespective of the subscripts α, β, γ. In such a case we say that G is $(h, 1)$ *isomorphic* (or *multiply isomorphic*) with K.

Concerning two such groups we have the

THEOREM 3. *The h operators of G which correspond to the identity of K, namely $S_{11}, S_{12}, \ldots, S_{1h}$, form an invariant subgroup of G.*

First, to prove that $S_{11}, S_{12}, \ldots, S_{1h}$ form a group H, consider any product $S_{1a}S_{1b}$. By the conditions of isomorphism, this product must be an operator in G of the set which corresponds to the operator $T_1T_1=E^2$ of K; that is, to E. Hence, there must be some subscript c such that $S_{1a}S_{1b}=S_{1c}$.

Next, to prove that H is invariant under G, we must show that $S^{-1}S_{1a}S$ belongs to H, where S is any operator of G. Let S correspond to T_b in K, and $S^{-1}S_{1a}S$ will

correspond to E, since $T_b^{-1}ET_b = E$. It follows that $S^{-1}S_{1a}S$ is to be found in the first line; i.e., it belongs to H.

EXERCISE

The linear group (6), § 7, is (2, 1) isomorphic with the collineation group $G = (E, A_2)$ given in the Example, § 10.

A linear group is always isomorphic with the corresponding collineation group.

33. **Factor group.** The group K of order $k = g/h$ discussed in the preceding paragraph, is called a *factor group* (or *quotient group*) of the group G of order g, and we write symbolically

$$K = G/H,$$

H being the invariant subgroup of G of order h which corresponds to the identity of K.

THEOREM 4. *Let G be a group of order g, containing an invariant subgroup H of order h. Then a factor group $K = G/H$ of $k = g/h$ operators can be constructed, to which therefore G is $(h, 1)$ isomorphic.*

To prove this theorem, we arrange the g operators of G in k lines as shown in table (1), § 28, the operators of H forming the first line.

Now, the h^2 products obtained by taking for a pre-factor in turn each of the h operators from a given line (the ath) and as a post-factor in turn each of the h operators from the same or another given line (the bth), will all fall in *one* line (say the cth; namely the line in which the product V_aV_b falls); symbolically $(HV_a)(HV_b) = HV_c$. This is easily seen in the following manner. Let (H) represent the phrase "an operator of H," and we have $(H)(H) = (H)$; and, since H is invariant under G, $V_a(H) = (H)V_a$. Consequently,

$$(H)V_a(H)V_b = (H)(H)V_aV_b = (H)V_c, \text{ if } V_aV_b = (H)V_c.$$

The reader may now readily prove that the symbols $H, HV_2, \ldots, HV_k$, looked upon as k distinct operators,

obey the conditions 1°—6°, § 25, as well as the additional condition for a finite group (§ 27). For instance, H satisfies the condition for the identity: $(H)(HV_a) = (HV_a)(H) = (H)V_a$. There is therefore at least one group of k operators $E, T_2, \ldots, T_k$ having the same multiplication table as these symbols (§ 47). Hence the existence of the factor group K, as a group of operators, is proved.

Exercises

1. Let G be a linear group in n variables, and H the group of similarity-transformations contained in G. The collineation group corresponding to G is a factor group G/H.

2. Prove that if the factor group K contains a subgroup K' of order k', then the corresponding hk' operators of G form a subgroup G' of G.

3. If K' of the preceding exercise is invariant under K, then G' is invariant under G.

4. Prove that the order of an operator of G is divisible by the order of the corresponding operator of K. (Hint: if S belongs to G and $S^n = E$, then the corresponding operator T of K satisfies the equation $T^n = E$.)

TWO SPECIAL TYPES OF GROUPS, §§ 34–35

34. An **abelian group** is a group G whose operators $E, S_2, \ldots, S_g$ are mutually commutative:

$$S_a S_b = S_b S_a. \tag{4}$$

The following two propositions are immediate consequences of (4):

(*a*) Every operator of an abelian group G, as well as every subgroup of G, is invariant under G.

(*b*) A factor group of an abelian group is again an abelian group.

Example.—Two invariant operators, A and B, of any group G are commutative, since $A^{-1}BA = B$. Hence, the invariant operators of G form an abelian self-conjugate subgroup of G (Exercise 4, § 31).

THEOREM 5. *An abelian group G of order g contains always a subgroup G' whose order g' is any given factor of g.*

In the proof of this theorem we shall adopt the process of complete induction. Accordingly, we assume the theorem true for any group K whose order k is less than the given number g, the order of the given group G for which the theorem is to be proved.

Let S be any operator of G. Assuming for the moment that its order h is a factor of g', we construct the group H of order h, consisting of S and its powers, and thereupon the factor group $K=G/H$. This factor group being abelian and having its order g/h less than g, it contains by assumption a subgroup K' of order g'/h, a factor of g/h. To K' will now correspond a subgroup of G of order g' (Exercise 2, § 33).

The proof of Theorem 5 thus depends on our finding an operator S in G whose order is a factor of g'. Now, the order n of any operator T chosen at random will either be prime to g', or will contain a factor h which divides g'. In the latter case the operator $T^{n/h}$ may be substituted for S of the proof, since it is of order h (§ 26, (*b*)).—In the first case let N be the group formed by T and its powers. The factor group G/N is of order g/n, a number which in the present instance is divisible by g'. This factor group therefore contains a subgroup of order g', and this again an operator whose order is a factor of g', say h (or g' itself). The order of a corresponding operator of G is a multiple of h (Exercise 4, § 33), and a power of this operator can therefore be taken for S, as shown above.

The abelian groups of order pq are simply isomorphic, p and q representing two distinct prime numbers. To take a special case, let $p=2$ and $q=3$. An abelian group of order 6 contains an operator, A, of order 2 and one, B, of order 3. The operator AB is of order 6 and will generate the group in question.

If $p=q$ the matter is different: there are two distinct types of abelian groups of order p^2. One type is generated by an operator of order p^2; and the other by two operators, both of order p. If $p=2$ the two types are as follows (S is of order 4, A and B both of order 2):

$$E,\ S,\ S^2,\ S^3;$$
$$E,\ A,\ B,\ AB.$$

35. **Groups whose orders are powers of a prime number.** The study of these groups is of the greatest importance for the theory of groups in general as well as for linear groups, particularly in view of Theorem 7. We shall here prove the following:

THEOREM 6. *A group G whose order is p^a, p being a prime number, contains p or more invariant operators, forming an invariant subgroup H. If G is not abelian, the abelian subgroup H is contained in a larger abelian subgroup G_1 which is invariant under G, though the operators of G_1 are not all separately invariant under G.*

1°. To prove the existence of H, we construct all the sets of conjugate operators of G (§ 29). If the number of sets that contain just one operator each (invariant operators) is h', and if the remaining sets contain respectively $g_2, \ldots, g_n$ operators, we have (cf. Exercise 5, § 30):

$$p^a = h' + g_2 + \ldots + g_n. \tag{5}$$

The numbers $g_2, \ldots, g_n$ are all powers of p, being factors of p^a and greater than unity. It follows that h' must be divisible by p. Hence, G contains at least p invariant operators, and all such operators form an abelian self-conjugate subgroup (Example, § 34), say of order p^b (Theorem 1, § 28). If G is abelian, $p^b = p^a$.

2°. To prove the existence of G_1, we now construct the factor group $K=G/H$ of order p^{a-b}. Treating this in the same way as G above, we find an abelian subgroup

K_1 consisting of invariant operators of K. Let T be any one of these except the identity, and let p^c be the order of that subgroup of K_1 formed by T and its powers. This subgroup is invariant under K, and the corresponding subgroup of G of order p^{b+c} is invariant under G (Exercise 3, § 33).

We have still to prove that this subgroup G_1 is abelian. By referring to the table (3), § 32, we see that G_1 is generated by H and one of those operators, V, of G corresponding to T of K. Now, all the operators of H are commutative with each other and with V, and the latter is commutative with any power of itself. The operators of G_1 are therefore mutually commutative.

EXERCISES

1. Prove that a group of order p^2 is abelian, and is therefore isomorphic with one of the types given in § 34.

2. The process above may be extended as follows: to K_1 corresponds an invariant subgroup H_1 of G; the factor group G/H_1 contains a subgroup consisting of invariant operators, and to this subgroup will correspond an invariant subgroup H_2 of G, etc. In this manner we shall obtain a series of subgroups of G:

$$H, H_1, H_2, H_3, \ldots, G.$$

Prove that each is an invariant subgroup of all that follow it, and that the factor groups $H_1/H, H_2/H_1, \ldots$, are abelian.

3. Prove that a group of order p^a contains a subgroup of order p^b, if $b<a$.

SYLOW'S THEOREM, §§ 36–39

36. In the case of a non-abelian group the sweeping statement of Theorem 5, § 34, is not generally true. But we can always predict a certain class of subgroups called **Sylow subgroups,** as stated in the following:

THEOREM 7. (*a*) *Let G be a group of order g, and let p be any prime factor of g. If p^a is the highest power of p*

that divides g, then there is in G at least one subgroup of order p^a. Denote this subgroup by P.

(b) If G contains more than one subgroup P, then all such subgroups are conjugate under G, and their number is of the form $1+pk$.

Proof of (a).—We adopt the process of complete induction, assuming that any group whose order is less than the given number g and is divisible by a power of p, say p^b, but by no higher power of p, contains a subgroup of order p^b. Two cases arise: 1°, G contains an invariant operator of order p; 2°, G contains no such invariant operator.

1°. Let S be an invariant operator of order p, and let H be the subgroup formed by S and its powers. Consider the factor group G/H. Its order is g/p, a multiple of p^{a-1}. By assumption, it has a subgroup of order p^{a-1}. To this subgroup corresponds a subgroup of G of order $p^{a-1}p=p^a$ (Exercise 2, § 33).

2°. Here there may or may not be invariant operators in addition to E in G whose orders are prime to p. All such operators form an abelian group H' (Exercise 4, § 31). The order, h', of this group is prime to p. For, otherwise H' would contain a subgroup of order p (Theorem 5, § 34), and the arguments of 1° would be valid.

We now construct all the complete sets of conjugate operators in G, and obtain an equation corresponding to (5), § 35:

$$g=h'+g_2+\ \ldots\ +g_n.$$

Evidently, the numbers $g_2, \ldots, g_n$ cannot all be multiples of p, since h' is not, whereas g is a multiple of p^a. Hence, at least one of the numbers $g_2, \ldots, g_n$, say g_2, is prime to p. If therefore S is an operator in this set of conjugates, we conclude by the aid of Theorem 2, § 29, that G contains a subgroup H of order $h=g/g_2$, a number

which is less than g and is divisible by p^a. By assumption, this group contains a subgroup of order p^a which is a subgroup of G, since H is a subgroup of G.

37. In the proof of (b) the following propositions are needed:

1°. An operator T of G of order p^a which transforms a Sylow subgroup P of G into itself ($T^{-1}PT=P$) belongs to P.

2°. If two different Sylow subgroups, P_1 and P_2, have in common a subgroup of order p^b, $b<a$ (cf. Exercise 6, § 27), then one of them is transformed into just p^{a-b} distinct groups of order p^a by the operators of the other.

To prove 1°, let m be the least positive number such that T^m belongs to P; in any event, $m\leqq p^a$. Then we can show that m is a factor of p^a; for if it is not, let q be the quotient and r the remainder when p^a is divided by m, so that $p^a-mq=r$; $r<m$. Then, since T^{p^a} and T^{mq} are both contained in P, it follows that T^r is also contained in P, contrary to the assumption as to T^m.

Therefore m is one of the numbers 1, p, p^2, . . . Assuming that T does not belong to P, let $m=p^\beta$. The group Q generated by T and the operators of P will now be of order $mp^a=p^{\beta+a}$, since it consists of all the operators

$$P,\ PT,\ PT^2,\ \ldots,\ PT^{m-1}.$$

(That these operators form a group of order mp^a is seen as follows: If we indicate the phrase "an operator of P" by the symbol (P), we have $T^s(P)=(P)T^s$, since $T^{-1}PT=P$, and therefore $((P)T^s)((P)T^t)=(P)(P)T^sT^t=(P)T^{s+t}$, so that the products of operators of the set Q are all contained in the set. Again, the mp^a operators are all distinct. For the p^a operators PT^s are all distinct; and the equation $(P)T^s=(P)T^t$ cannot be true unless $(P)=T^{t-s}$; that is, unless $s=t$.)

But G cannot contain a subgroup Q of order $p^{\beta+a}$ (Theorem 1, § 28). Hence, T must belong to P.

To prove 2°, let H be the subgroup of order p^b common to the two groups P_1 and P_2. By 1°, no operator of P_1 except those of H transform P_2 into itself. We now adopt the process employed in the proof of Theorem 2, § 29: we arrange the operators of P_1 in the form of the table (1), § 28, the first line consisting of the operators of H. To each line of the table there will then correspond a distinct group conjugate to P_2, making in all $p^a/p^b = p^{a-b}$ distinct groups.

38. *Proof of* (*b*).—Consider a set of conjugate Sylow subgroups of order p^a:

$$P_1,\ P_2,\ \ldots,\ P_n. \tag{6}$$

By 2°, § 37, the operators of P_1 will transform P_2 into p^{a-b} distinct groups. If the set contains other groups in addition to these p^{a-b} and P_1, then the operators of this group (P_1) will transform one of them into say p^{a-c} groups distinct from those already counted. Proceeding thus, we find

$$n = 1 + p^{a-b} + p^{a-c} + \ldots = 1 + pk,$$

since p^{a-b}, p^{a-c}, . . are all multiples of p.

Now, if G contained another set $P_{n+1}, \ldots, P_m$ of conjugate Sylow subgroups, their number would likewise be of the form $1+pk'$. On the other hand, P_1 is not a member of this new set. We can therefore show that the number of groups in the set is a multiple of p, say pk'', in the same manner as the number of groups $P_2, \ldots, P_n$ were shown to be a multiple of p. But, the equation $1+pk' = pk''$ is impossible. It follows that (6) is the only set of Sylow subgroups contained in G, and (*b*) is fully proved.

EXERCISES

1. Prove that a group G whose order is divisible by p^b contains a subgroup of order p^b. (Cf. Exercise 3, § 35.)

2. If the largest subgroup H that P_1 can have in common with another Sylow subgroup is of order p^b, prove that the number of Sylow subgroups in G of order p^a is of the form $1+p^{a-b}k$.

3. Show that a group of order 40 contains a single Sylow subgroup of order 5, which is therefore an invariant subgroup.

4. Prove that a group of order pq is abelian, if p and q are prime numbers such that $p-1$ is not divisible by q, nor $q-1$ divisible by p.

39. We conclude by proving the following useful theorem:

THEOREM 8. *A subgroup of G of order p^b is always contained in at least one Sylow subgroup of order p^a.*

Let K be a subgroup of order p^b, and assume it is not contained completely in any one of the groups P_1, P_2, . . . , P_n, § 38. Then, arranging these in sets of conjugates with respect to the operators of K, we find that the number of groups in the set is a multiple of p, as would be the case with the number of groups in the tentative set P_{n+1}, . . . , P_m, § 38. But this is impossible by Theorem 7, (*b*).

B. SUBSTITUTION GROUPS

40. **Definitions.** (*a*) A *substitution* (or *permutation*) S on a given set of letters a_1, a_2, a_3, . . . , a_n is the operation of replacing these letters respectively by a_p, a_q, a_r, . . . , a_w, with the understanding that the subscripts $p, q, r, \ldots, w$ are the subscripts 1, 2, 3, . . . , n over again in the same or a different order.* We shall temporarily indicate such a substitution by the symbol

$$S=\begin{pmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_p & a_q & a_r & \ldots & a_w \end{pmatrix} \tag{7}$$

* The letters are generally involved in one or more given functions, as $a_1x_1+a_2x_2+a_3x_3+\ \ldots\ +a_nx_n$. This function would be transformed into $a_px_1+a_qx_2+a_rx_3+\ \ldots\ +a_wx_n$ by the substitution S above.

The phrases "replace a by b," "put b in place of a," "change a into b" are to be regarded as synonymous.

The columns may evidently be changed about in any manner so long as a_p falls below a_1, a_q below a_2, etc.; and two substitutions are equal if their columns are equal aside from the order in which they are written. For instance,

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ a_2 & a_3 & a_1 \end{pmatrix} = \begin{pmatrix} a_2 & a_1 & a_3 \\ a_3 & a_2 & a_1 \end{pmatrix} \neq \begin{pmatrix} a_1 & a_2 & a_3 \\ a_1 & a_3 & a_2 \end{pmatrix}.$$

(*b*) The *product* ST of two substitutions

$$S = \begin{pmatrix} a_1 & a_2 & a_3 & . & . & a_n \\ a_p & a_q & a_r & . & . & a_w \end{pmatrix}, \qquad T = \begin{pmatrix} a_p & a_q & a_r & . & . & a_w \\ a_\alpha & a_\beta & a_\gamma & . & . & a_\lambda \end{pmatrix},$$

is the substitution resulting from carrying out the two substitutions successively, first S and then T:

$$ST = \begin{pmatrix} a_1 & a_2 & a_3 & . & . & a_n \\ a_\alpha & a_\beta & a_\gamma & . & . & a_\lambda \end{pmatrix}.$$

With this rule for multiplication, the associative law: $S(TU) = (ST)U$, is readily found to be true.

(*c*) *The identity* is the substitution in which each letter is replaced by itself:

$$E = \begin{pmatrix} a_1 & a_2 & . & . & a_n \\ a_1 & a_2 & . & . & a_n \end{pmatrix}.$$

(*d*) The *inverse* of the substitution S is the substitution

$$S^{-1} = \begin{pmatrix} a_p & a_q & a_r & . & . & a_w \\ a_1 & a_2 & a_3 & . & . & a_n \end{pmatrix}.$$

In consequence of these definitions and propositions, the totality of substitutions on n letters $a_1, a_2, \ldots, a_n$ form a class O of operators (§ 25).

41. **Permanent notation.** A simpler notation for a substitution S than that employed in (7), § 40, may be developed as follows. Writing down the letter a_1 we follow with the letter that takes its place, namely a_p; then

we follow with the letter that replaces a_p, say a_α; and so on: $a_1 a_p a_\alpha \ . \ . \ .$ There being a finite number of letters, we must sooner or later arrive at a letter that has already been written. The first one to be thus duplicated must be a_1; for, if it were some other letter, say a_p, the lower line $a_p a_q \ . \ . \ a_w$ of the substitution S in (7) would plainly have to contain a_p at least twice, whereas the letters of this line are the n different letters $a_1 a_2 \ . \ . \ a_n$ in some order, once each.

Let therefore the last letter to be written down before a_1 reappears be a_m. We then have a *cycle*

$$(a_1 a_p a_\alpha \ . \ . \ . \ a_m).$$

If this cycle does not exhaust the n letters under consideration, we start with a new letter and proceed as above, forming a new cycle, which may be written immediately after the first; and so on. No one letter will appear in two different cycles, as otherwise such a letter would have to appear at least twice in the lower line of (7). It is customary to exclude all cycles which contain just one letter, such a letter remaining unchanged by S. Thus the substitution

$$S = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_1 & a_3 & a_4 & a_2 & a_6 & a_5 \end{pmatrix}$$

is written $S = (a_2 a_3 a_4)(a_5 a_6)$.

Exercises

1. Show that if $S = \begin{pmatrix} a_1 a_2 a_3 a_4 a_5 \\ a_2 a_3 a_4 a_5 a_1 \end{pmatrix}$, and $T = \begin{pmatrix} a_1 a_2 a_3 a_4 a_5 \\ a_1 a_3 a_2 a_5 a_4 \end{pmatrix}$, then $S^5 = E = T^2$.

Show also that in the permanent notation, $S = (a_1 a_2 a_3 a_4 a_5)$, $T = (a_2 a_3)(a_4 a_5)$, and that $ST = (a_1 a_3 a_5)$, $TS = (a_1 a_2 a_4)$.

2. The substitution $(a_2 a_3 a_4)(a_5 a_6)$ is the product of the substitutions $(a_2 a_3 a_4)$ and $(a_5 a_6)$. Prove that a substitution consisting of a number of cycles is equal to the product of the substitutions

represented by the individual cycles, and that these factors are commutative.

3. Show that the inverse of the cycle $(a_1a_2 \ . \ . \ a_{n-1}a_n)$ is the cycle $(a_na_{n-1} \ . \ . \ a_2a_1)$, and that the inverse of a substitution consisting of a number of cycles is the substitution consisting of the inverses of those cycles.

4. Show that the order of the operator consisting of a single cycle containing n letters is n. Hence prove that the order of a substitution composed of several cycles containing respectively $n_1, n_2, \ . \ .$ letters, is the least common multiple of the numbers $n_1, n_2, \ . \ . \ .$ (Illustration: the order of $(a_2a_3a_4)(a_5a_6)$ is 6.)

5. The order of ST in Exercise 1 above is 3, and the cycles in S and T contain respectively 5 and (2, 2) letters. Do these facts agree with the statements in Exercise 4?

42. **Even and odd substitutions.** A cycle of k letters is equal to the product of $k-1$ cycles of 2 letters each (called *transpositions*):

$$(a_1a_2a_3 \ . \ . \ a_k) = (a_1a_2)(a_1a_3) \ . \ . \ . \ (a_1a_k).*$$

We therefore classify substitutions into *even* or *odd* substitutions according to whether they are equal to a product of an even or an odd number of transpositions. For instance, the substitution $(a_1a_2a_3)(a_4a_5a_6a_7)$ is odd, since it can be written as the product $(a_1a_2)(a_1a_3)(a_4a_5)(a_4a_6)(a_4a_7)$.

This classification is justified since, no matter in which one of the infinite number of possible ways a given substitution can be written as a product of transpositions, it is either always even or always odd. To prove this statement, consider the following function:

$$f = (a_1-a_2)(a_1-a_3) \ . \ . \ (a_1-a_n)(a_2-a_3) \ . \ . \ (a_2-a_n) \ . \ . \ (a_{n-1}-a_n),$$

* Note that the letter a_1 is common to all the transpositions. Hence, this is not the normal notation for a substitution as developed in § 41. The laws deduced in Exercises 3 and 4 are therefore not applicable to the form above.

namely the product of all the possible differences of the n letters involved. This function changes sign when operated upon by a single transposition, and hence also when operated upon by an odd substitution, but remains unchanged in value when operated upon by an even substitution.

43. Substitution groups. Symmetric and alternating groups. A set of g different substitutions form a *substitution group* of order g if the product of any two substitutions of the set, whether equal or not, is again a substitution of the set. Cf. § 27, where such a group is given in Example 2. In our present notation this group is written as follows:

$$E,\ (ab)(cd),\ (ac)(bd),\ (ad)(bc). \tag{8}$$

All the $n!$ permutations on n letters evidently form a group, called the *symmetric group* on the given letters. Thus, the symmetric group on 3 letters a, b, c is of order 6 and is composed of the substitutions E, (abc), (acb), (ab), (ac), (bc).

It is plain that the totality of the even substitutions contained in the symmetric group G on n letters form by themselves a group, called the *alternating group.* Its order is one-half that of the corresponding symmetric group. For, let there be p even and q odd substitutions in G. The $p+q$ products obtained by multiplying each of these substitutions by a given transposition must produce the same $p+q$ substitutions over again (Exercise 3, § 27) with this difference, that we now have p odd and q even substitutions. Hence $p=q$.

Inside a given symmetric group, the conjugate of an even substitution is again an even substitution. It follows that the alternating group is invariant (§ 31) under

the corresponding symmetric group. The alternating group on 5 or more letters is always a simple group (§ 49).

EXERCISE

Construct the symmetric and alternating groups on 4 letters a, b, c, d. Show that the latter contains a single Sylow subgroup of order 4, namely the group (8), and that the former contains 3 Sylow subgroups of order 8, which all contain the group (8).

44. **Transitivity and intransitivity.** If the letters of a substitution group break up into two or more sets having no letters in common, such that no substitution will replace a letter of one set by a letter of another, then the group is said to be *intransitive*. Otherwise the group is *transitive*.

The transitive groups are further subdivided into *primitive* and *imprimitive* groups. If the letters break up into two or more sets of such a nature that the letters of any one set are either all replaced by letters of the same set, or are all replaced by letters of another set, then the group is imprimitive. If no such division is possible, the group is primitive.

Examples.—The group (8), § 43, is transitive, while the group E, $(ab)(cd)$, is intransitive. The two sets of letters, (a, b) and (c, d) are called *systems* (or *sets*) *of intransitivity*.

The transitive group (8), § 43, is imprimitive. Its two *systems of imprimitivity* may be selected in three ways: 1°: (a, b), (c, d); 2°: (a, c), (b, d); 3°: (a, d), (b, c). The symmetric group on three or more letters is primitive.

45. We proceed to prove the following important theorem concerning transitive groups:

THEOREM 9. *Let G be a transitive substitution group of order g on n letters $a_1, a_2 \ . \ . \ , a_n$. Then,*

(a) there is in G a substitution which replaces any given letter, say a_1, by any other given letter;

(b) all those substitutions in G which leave unchanged a given letter, say a_1, form a subgroup of order g/n.

Proof.—(*a*) Let us assume that $a_1, a_2, \ldots, a_m$ ($m<n$) are the letters into which a_1 is changed by the various substitutions of G. Then none of these m letters can be replaced by one of the remaining letters $a_{m+1}, \ldots, a_n$; or vice versa. For, let V_2 change a_1 into a_2, and assume that there is a substitution T which changes a_2 into a_{m+1}; then the substitution V_2T would change a_1 into a_{m+1}, contrary to what was stated in regard to the first m letters. Again, if the substitution T_1 changed one of the last $n-m$ letters into one of the first m letters, then T_1^{-1} would do the reverse. But this has just been proved impossible.

Now, a transitive group cannot contain two such sets of letters. Accordingly, G must contain a substitution (V_2) which replaces a_1 by a_2, one (V_3) which replaces a_1 by a_3, etc., and finally one (V_n) which replaces a_1 by a_n.

(*b*) Let all those substitutions which leave a_1 unchanged constitute a set $H=(S_1, S_2, \ldots, S_h)$, then H is a group. For, the products S_aS_b all belong to H.

To find the order of H, we arrange the hn substitutions $H, HV_2, HV_3, \ldots, HV_n$ in the form of the table (1), § 28. The h substitutions in any one line are evidently all distinct (since $S_aV_c=S_bV_c$ would necessitate $S_a=S_b$); moreover the substitutions of two different lines are distinct, since those in the line HV_c all replace a_1 by a_c. Finally, any substitution of G must occur in our table. For, if T replaces a_1 by a_c, then TV_c^{-1} belongs to H, say $TV_c^{-1}=S_a$, so that $T=S_aV_c$. Hence, $g=hn$, or $h=g/n$.

C. On the Representation of a Group of Operators as a Substitution Group

46. **Theorem 10.** *A group of operators G which contains a conjugate set of n subgroups (or operators) is simply or multiply isomorphic* (§ 32) *with a transitive substitution group on n letters.*

1°. If the n subgroups (or operators) are designated $a_1, a_2, \ldots, a_n$, we construct a substitution group K on the n letters $a_1, a_2, \ldots, a_n$, isomorphic with G, in the following manner. Let S be any given operator of G, and let us suppose that it transforms the group (operator) a_1 into a_p, a_2 into a_q, etc.:

$$S^{-1}a_1S=a_p,\ S^{-1}a_2S=a_q,\ \ldots,\ S^{-1}a_nS=a_w.$$

Then the subscripts $p, q, \ldots, w$ are all different and must be the subscripts 1, 2, . , n over again in some order. Accordingly, we can construct a substitution as follows (using the notation of § 40):

$$T=\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_p & a_q & \ldots & a_w \end{pmatrix},$$

and we shall associate this substitution with S.

2°. To the g operators $S_1, S_2, \ldots$ of G thus correspond g substitutions $T_1, T_2, \ldots$ of a set K; and to prove that these substitutions form a group isomorphic with G it is sufficient to prove that if $S_aS_b=S_c$, then $T_aT_b=T_c$ (§§ 27, 32). Now, if S_a transforms a group (operator) a' into the group (operator) a'', and S_b transforms a'' into a''', then S_c transforms a' into a''':

$$\begin{aligned} S_c^{-1}a'S_c=(S_aS_b)^{-1}a'(S_aS_b)&=S_b^{-1}(S_a^{-1}a'S_a)S_b \\ &=S_b^{-1}a''S_b=a'''. \end{aligned}$$

Again, if T_a replaces a' by a'', and T_b replaces a'' by a''', then $T_c=T_aT_b$ replaces a' by a'''. The isomorphism is therefore established.

3°. If now the g substitutions obtained above are all distinct, the isomorphism is simple. If, on the other hand, we find that several operators $S_{a1}, S_{a2}, \ldots, S_{ah}$ correspond to a single substitution T_a, then G is multiply isomorphic with the group K' composed of the totality of

distinct substitutions in K. For, arranging the operators of G into sets in such a manner that all those operators furnishing the same substitution are thrown into one set, we find that these sets contain the same number of operators.

Thus, the h operators $S_{a_1}S_{a_1}^{-1}$, $S_{a_2}S_{a_1}^{-1}$, . . . , $S_{a_h}S_{a_1}^{-1}$ all correspond to the identity $T_aT_a^{-1}=E$; and conversely, if $S_{11}, S_{12}, \ldots, S_{1h}$ all correspond to the identity E, then the operators $S_{a_1}S_{11}$, $S_{a_1}S_{12}$, . . . , $S_{a_1}S_{1h}$ all correspond to one and the same substitution $T_aT_1=T_a$.

4°. Finally, to prove that the substitution group thus constructed is transitive, we note that within G the groups (operators) a_1, a_2, . . a_n form a complete conjugate set, so that there is an operator in G which transforms a_1 into any given group (operator) a_p. There is therefore within K a substitution which replaces the letter a_1 by the letter a_p.

COROLLARY. *If a simple group* (§ 31) *G contains a set of n conjugate subgroups (or operators), then we can construct a transitive substitution group on n letters which is simply isomorphic with G.*

EXERCISES

1. The linear group (7), § 7, contains a conjugate set of two operators, B_2 and B_4. Construct a substitution group which is (1, 4) isomorphic with the given group.

2. The collineation group of Exercise 2, § 12, contains a set of three conjugate operators, namely the 2d, 3d, and 6th. Show that the given collineation group is simply isomorphic with the symmetric group on three letters.

3. Let p, q, r, s denote the four subgroups of order 3 contained in the symmetric group G on four letters a, b, c, d. Construct the transitive substitution group on the letters p, q, r, s, isomorphic with G.

47. Theorem 11. *A group G of order g can be represented as a transitive substitution group H on g letters*

(called a regular substitution group). In this representation, every substitution except the identity, will replace every letter by a different letter.

The group (8), § 43, is regular.

Let the operators of G, as well as the letters of substitution, be denoted by T_1 (or E), T_2, . . . , T_g. We now associate with an operator T_p of G the substitution

$$S_p = \begin{pmatrix} T_1 & T_2 & . & . & T_g \\ T_1' & T_2' & . & . & T_g' \end{pmatrix}, \tag{9}$$

where T_a' is the letter which in G represents the operator T_aT_p; i.e., $T_a' = T_aT_p$. (Cf. § 40; the symbol making up the right-hand member of (9) is actually a "substitution," since the letters in the lower line are the letters in the upper line written in some order (Exercise 3, § 27).)

In no case is $T_a' = T_a$ unless $T_p =$ the identity $= T_1$; and then every $T_a' = T_a$, so that S_1 becomes the identity. Furthermore, no two substitutions corresponding to different operators can be equal (from $T_aT_p = T_bT_p$ follows $T_a = T_b$). Hence, if we find that $S_pS_q = S_r$ whenever $T_pT_q = T_r$, the substitutions S_1, . . . , S_g form a group H, simply isomorphic with G, and fulfilling the conditions of the theorem if it is transitive.

Now, since the series T_1, T_2, . . . , T_g is equivalent to the series T_1T_k, T_2T_k, . . . , T_gT_k, aside from the order, the substitution S_q may equally well be written

$$S_q = \begin{pmatrix} T_1T_k & . & . & T_gT_k \\ T_1T_kT_q & . & . & T_gT_kT_q \end{pmatrix},$$

which we shall abbreviate to $(T_aT_k,\ T_aT_kT_q)$. We then have

$$\begin{aligned} S_pS_q &= (T_a,\ T_aT_p)(T_aT_p,\ T_aT_pT_q) = (T_a,\ T_aT_pT_q) \\ &= (T_a,\ T_aT_r) = S_r, \end{aligned}$$

and the isomorphism is proved.

The group H will be transitive if there is a substitution which replaces T_1 by any given letter T_n. Now, the substitution $S_n = (T_a,\ T_a T_n)$ does that. The theorem is therefore proved.

EXERCISE

Construct the regular substitution group on 6 letters $x_1, x_2, \ldots, x_6$, isomorphic with the symmetric group on 3 letters.

D. On Simple Groups

48. In later chapters it will be of great convenience for us to use a number of known results about simple groups. Some of these results shall merely be stated here without proof; in the case of the theorems 12 and 13 the proofs are outlined for the benefit of advanced students. The detailed analysis would be somewhat lengthy and in part difficult.

We begin by enumerating the simple groups whose orders are not greater than 2000* or that can be represented as substitution groups on not more than 10 letters:†

(*a*) the alternating groups on 5, 6, . . . , 10 letters (§ 49);

(*b*) certain groups of orders 168, 504, 660, 1092.

49. **Theorem 12.** *The alternating substitution group of order $n!/2$ on n letters is a simple group when $n \geqq 5$.*

Outline of proof.—1°. If a group on n letters $a_1, \ldots, a_n$ contains all the substitutions of the form $(a_p a_q a_r)$, it is the alternating group.

* Hölder, *Mathematische Annalen*, XL (1892), 55; Cole, *American Journal of Mathematics*, XIV (1892), 378, XV (1893), 303; Burnside, *Proceedings of the London Mathematical Society*, XXVI (1895), 333; Ling and Miller, *American Journal of Mathematics*, XXII (1900), 13.

Strictly speaking, a group whose order is a prime number is a simple group, having no invariant subgroups. But such groups will not be included under the concept "simple groups" in succeeding chapters.

† Jordan, *Comptes Rendus*, LXXV (1872), 1754.

2°. A possible self-conjugate subgroup of the alternating group which contains a substitution S must contain the substitution $U=S^{-1}T^{-1}ST$, where T is any substitution in the alternating group. Now, whatever form S may have, it is always possible to find such a substitution T that U is composed of the single cycle $(a_p a_q a_r)$.

3°. All the conjugates to U with respect to the substitutions of the alternating group must be contained in the self-conjugate subgroup. But these conjugates are indeed all the possible substitutions composed of just a single cycle of three letters each; and therefore, by 1°, the proposed self-conjugate subgroup is the alternating group itself.

50. **Theorem 13.*** *The alternating group on n letters is simply isomorphic with the group generated by the* $n-2$ *operators* $F_1, \ldots, F_{n-2}$ *which satisfy the relations:*

$$F_1^3=E, \quad F_2^2=F_3^2= \ldots =F_{n-2}^2=E;$$
$$(F_1F_2)^3=(F_2F_3)^3= \ldots =(F_{n-3}F_{n-2})^3=E;$$
$$(F_aF_b)^2=E \quad (a=1, 2, \ldots, n-4; \ b=a+2, a+3, \ldots, n-2).$$

Outline of proof.—1°. Adopting the process of complete induction, we assume that $F_1, \ldots, F_{n-3}$ generate a group H simply isomorphic with the alternating group on $n-1$ letters (we take $n>3$; for $n=3$ the theorem is self-evident). Hence, the following symbols:

$$R_n, \ R_{n-1}, \ \ldots, \ R_1, \tag{10}$$

where

$$R_{n-1}=H, \ R_k(k<n-1)=HF_{n-2}F_{n-3} \ldots F_k, \ R_n=R_1F_1,$$

represent at most $[(n-1)!/2]n=n!/2$ operators.

* E. H. Moore, *Proceedings of the London Mathematical Society*, XXVIII, No. 596. The outline given above is of the proof given by L. E. Dickson, *Linear Groups* (Leipzig, 1901), pp. 289–90.

2°. The symbols (10) contain all the operators generated by $F_1, \ldots, F_{n-2}$. For, the set (10) is reproduced if we multiply on the right by any one of these operators, and therefore also by any operator generated by them. Accordingly, the group G generated by $F_1, \ldots, F_{n-2}$, is of order $n!/2$ at most.

3°. Now, the substitutions $F_1' = (a_1a_2a_3), F_2' = (a_1a_2)(a_3a_4), F_3' = (a_1a_2)(a_4a_5), \ldots, F_{n-2}' = (a_1a_2)(a_{n-1}a_n)$ satisfy the relations imposed upon the corresponding operators of the theorem. It follows that G is isomorphic with the substitution group G' generated by $F_1', \ldots, F_{n-2}'$. But this is the alternating group on n letters, and is of order $n!/2$.

4°. Finally, the order of G being at most $n!/2$ by 2°, it follows that G and G' are simply isomorphic.

CHAPTER III

THE LINEAR GROUPS IN TWO VARIABLES

51. General remarks on linear groups and collineation groups.

1°. A collineation group may readily be exhibited as a linear group, and vice versa, as shown in §§ 9, 10, 12. It is therefore necessary to discuss only one of these categories, preferably the latter, which lends itself more readily to study. Accordingly, it will be our practice to apply the descriptive terms of chap. ii, (A), to a group under consideration, with reference to this group as written in linear form. For instance, we shall say that the group (7), § 7, is non-abelian, though the corresponding collineation group (E, A_1, B_1, B_2) is abelian. Moreover, certain terms have reference to linear groups only, namely (in)transitivity (§ 14), (im)primitivity, and monomial form (§ 60).

On the other hand, a group is generally (in the literature) described as *simple* if the corresponding collineation group is simple; that is, when classifying the groups in a given number of variables, we put into the class "simple groups" all the linear groups which are simple, together with those whose factor groups G/H are simple, H representing the group of similarity-transformations contained in G. But this is the only exception to the practice agreed upon.

2°. It will, furthermore, be our practice to write a linear group in such a way that the transformations all have a determinant unity. Of course, if G (or a subgroup of G) is intransitive, then a constituent of this group embracing one or more sets of intransitivity may not be

subject to this rule. An instance is furnished by an abelian group written in canonical form: (α, α^{-1}). Here the groups in one variable, say $x=\alpha x'$, do not have unity for the value of their determinants.

3°. It is often convenient to write the order of a group G in the form $g\phi$ (after Jordan), where g represents the order of the collineation group corresponding to G, and ϕ (not specified) the order of the group of similarity-transformations contained in G. For example, the order of the group (7), § 7, may be written either 8 or 4ϕ.

We may, correspondingly, write the order of a linear transformation S in the form $g\phi$, this being the order of the group generated by S. Thus, 2ϕ is the order of the transformation $(i, -i)$, where $i=\sqrt{-1}$. If the order of the transformation $S=(\alpha, \beta)$ is $g\phi$, that of the transformation $T=(1, \beta/\alpha)$ is g.

Obviously we write a linear group in such a way that ϕ is as small as possible, under the condition specified in 2°. In the case of the groups in two variables, $\phi=2$, except in one instance, since a collineation of order 2 cannot be written in the form of a linear transformation of determinant unity unless it has the form $(i, -i)$, where $i=\sqrt{-1}$. A group of even order must therefore contain the group of similarity-transformations $E=(1, 1)$, $E_1=(-1, -1)$. The exception mentioned is an abelian group of odd order.

4°. *Equivalence.*—A group is said to be *equivalent* to all the groups which flow from it by means of a change of variables. If the groups K_1 and K_2 are equivalent, then there is a linear transformation T such that $T^{-1}K_1T=K_2$ (§ 13). Two groups equivalent to a third are equivalent to each other (cf. § 30).

52. **The linear groups in two variables: mode of attack.** There are several processes available for the determination of the different non-equivalent groups in

two variables.* We shall here employ a modified form of Klein's original process, for the sake of its historical and geometrical interest. An outline of this process follows.

1°. Any given transformation S of a group G in the variables x_1, x_2, whose Hermitian invariant is $I = x_1\bar{x}_1 + x_2\bar{x}_2$ can be written as a product $S = S_1S_2S_3$,† where S_1 and S_3 have the canonical form:

$$S_1 = (\cos u - i \sin u,\ \cos u + i \sin u),$$
$$S_3 = (\cos w - i \sin w,\ \cos w + i \sin w), \text{ and}$$

$$S_2 = \begin{bmatrix} \cos v & \sin v \\ -\sin v & \cos v \end{bmatrix}.$$

The transformation $\bar{S}$ of the group $\bar{G}$ conjugate-imaginary to G is similarly equal to the product $\bar{S}_1\bar{S}_2\bar{S}_3$, where

$$\bar{S}_1 = (\cos u + i \sin u,\ \cos u - i \sin u),$$
$$\bar{S}_3 = (\cos w + i \sin w,\ \cos w - i \sin w),$$

$$\bar{S}_2 = S_2. \qquad (\S\ 53)$$

We shall denote by H the intransitive group whose constituents are G and $\bar{G}$; that is, the group whose variables are x_1, x_2, $\bar{x}_1$, $\bar{x}_2$. In these variables let T, T_1, T_2, T_3 denote the transformations corresponding to S, S_1, S_2, S_3, and we have $T = T_1T_2T_3$.

2°. Now let the three real functions $X = x_1\bar{x}_1 - x_2\bar{x}_2$, $Y = x_1x_2 + x_2\bar{x}_1$, $Z = (x_1\bar{x}_2 - x_2\bar{x}_1)\sqrt{-1}$ denote rectangular co-ordinates in space. The transformations T_1, T_2, T_3

* Klein, *Mathematische Annalen*, IX (1876), 183 ff.; *Vorlesungen über das Ikosaeder*, Leipzig, 1884, pp. 116–20; Gordan, *Mathematische Annalen*, XII (1877), 23 ff.; Jordan, *Journal für die reine und angewandte Mathematik*, LXXXIV (1878), 93–112; *Atti della Reale Academia di Napoli*, VIII (1879); Fuchs, *Journal für die reine*, etc., LXXXI, LXXXV (1876, 1878), 97, 1 ff.; Valentiner, *De endelige Transformations-Gruppers Theori*, Copenhagen, 1889, pp. 100 ff.

† The transformations S_1, S_2, S_3 are not *separately* transformations of G.

are then shown to represent real rotations around the $X-$, $Z-$, $X-$axes respectively. It follows by a well-known theorem that T is a real rotation around a certain axis which passes through the origin. There results a group G' of rotations in space which is isomorphic with G (§ 54).

3°. Since the rotations of G' leave the origin fixed, they must transform into itself a sphere Σ whose center is the origin. If now R be an axis of rotation and if P_1 be one of the points where R cuts Σ, then P_1, and all the points $P_2, \ldots, P_t$ into which P_1 is transformed by the rotations of G' will be the vertices of a regular polyhedron (including the limiting cases where there is a single axis of rotation or where the polyhedron becomes a flat polygon) (§ 55).

4°. The groups of rotations (G') may now be constructed to correspond to the regular polyhedra. We find five types, and correspondingly five non-equivalent linear groups (G) (§§ 56–58).

53. *Proof of 1°.*—The transformation S has the unitary form and its determinant is unity. We may therefore write (cf. Exercise 1, § 20):

$$S=\begin{bmatrix} a & b \\ -\bar{b} & \bar{a} \end{bmatrix}, \qquad a\bar{a}+b\bar{b}=1.$$

Let p and q represent the positive square roots of the real positive numbers $a\bar{a}$ and $b\bar{b}$ respectively, and we have $p^2+q^2=1$. Accordingly, we can write $p=\cos v$, $q=\sin v$. Moreover, $|a/p|=1$ and $|b/q|=1$, so that we may write

$$a/p=\cos h-i\sin h, \qquad b/q=\cos k-i\sin k;$$
$$\bar{a}/p=\cos h+i\sin h, \qquad \bar{b}/q=\cos k+i\sin k.$$

If we finally put $h=u+w$, $k=u-w$, we obtain by direct multiplication

$$S_1S_2S_3=S.$$

54. *Proof of 2°.*—The functions X, Y, Z will be transformed by T_1, T_2, T_3, defined in 1°, into linear functions of themselves. In fact, we may readily prove that

$$(X)T_1 = X, \quad (Y)T_1 = Y \cos 2u - Z \sin 2u,$$
$$(Z)T_1 = Y \sin 2u + Z \cos 2u,$$

with similar results for T_2 and T_3.

We can exhibit these results in a different form. Looking upon T_1, T_2, T_3 as linear transformations in the variables X, Y, Z, they will appear as follows:

T_1: $X = X'$, $\quad Y = Y' \cos 2u - Z' \sin 2u$,
$\quad Z = Y' \sin 2u + Z' \cos 2u$;

T_2: $X = X' \cos 2v + Y' \sin 2v$, $\quad Y = -X' \sin 2v + Y' \cos 2v$,
$\quad Z = Z'$;

T_3: $X = X'$, $\quad Y = Y' \cos 2w - Z' \sin 2w$,
$\quad Z = Y' \sin 2w + Z' \cos 2w$.

If we interpret X, Y, Z as rectangular co-ordinates in ordinary space, we recognize here three real rotations around the $X-$, $Z-$, $X-$axes respectively. These rotations, performed successively, are equivalent to a single rotation T.

To the different transformations (S) of G will in this manner correspond rotations (T) of a group G', isomorphic with G. The isomorphism is (1, 2) in case G contains the transformation $E_1 = (-1, -1)$, since both this transformation and the identity $(E = (1, 1))$, and no others, give rise to the single rotation $E' = (1, 1, 1)$, and vice versa.

55. *Proof of 3°.*—Consider the sphere Σ together with all of the axes of rotations of G'. A rotation B of G' will permute these axes among themselves; in fact, the axis of a rotation A is by B transformed into the axis of the rotation $B^{-1}AB$. Accordingly, if P_1 is the extremity

of an axis of period m (that is, an axis whose corresponding angles of rotation are the different multiples of $360°/m$), then the points $P_1, P_2, \ldots, P_t$ into which P_1 is transformed by the various rotations of G' will be extremities of axes of period m, and the distribution of these points about any one of them is similar to the distribution about any other.

Now, if $t>1$, let arcs of great circles be drawn connecting P_1 with all the points $P_2, \ldots, P_t$, and let the shortest arc be of length L. The number of arcs of this length radiating from P_1 is m or a multiple of m, since always m of the arcs are interchanged by rotations about the axis through P_1. However, there cannot be more than 5 such arcs, unless $L=180°$. For, if there were 6 or more, a pair of them, say C_s, C_r, would make an angle $\theta \leqq 60°$ with each other at P_1; and, this being the case, the arc L' connecting P_s and P_r (the points of $P_2, \ldots, P_t$ located on C_s and C_r) would have a length $<L$. For, by trigonometry,

$$\cos L' = \cos^2 L + \sin^2 L \cos\theta \geqq \cos^2 L + \tfrac{1}{2}\sin^2 L$$
$$= \tfrac{1}{2}(1+\cos^2 L) > \cos L;$$

and, since $0<L'<90°$, it follows that $L'<L$. But this is contrary to hypotheses, since the lengths of the arcs radiating from P_s are equal to the lengths of the arcs radiating from P_1. Similarly we may prove that an arc of length L joining two of the points $P_1 \ldots P_t$ cannot intersect another arc of the same nature.

Let $m>2$. Then it follows that there are just m arcs of length L radiating from P_1, each making an angle of $360°/m$ with its adjacent arcs. The same is true for each of the points $P_2, \ldots, P_t$, and we see that the sphere will be divided by all the arcs of length L, joining the various points $P_1 \ldots P_t$ which can be reached from one of them by passing along such arcs, into a number of

equal and regular polygons. Accordingly, these points are the vertices of a regular polyhedron inscribed in Σ.

The diameters of Σ passing through the middle points of the arcs L and through the middle points of the regular polygons will either coincide with the axes already obtained or will be additional axes of rotations of G'.

Next, let there be no axis of period greater than 2. If there are two axes of period 2, say A_1 and A_2, cutting each other under an angle α which may be assumed $\leqq 90°$, then a rotation of 180° around A_1 followed by a rotation of 180° around A_2 is equivalent to a rotation of 2α around an axis perpendicular to the plane of A_1 and A_2. Hence 2α is a multiple of 180°; i.e., $\alpha = 90°$. It follows that we have just one axis of period 2, or just three such which are mutually perpendicular.

THE GROUPS OF THE REGULAR POLYHEDRA, §§ 56–58

56 (4°). **Limiting cases.** In order to tabulate the linear groups (G) we may proceed as follows. From the geometrical data given the analytical equivalents of the rotations of G' can be calculated, and then we can reverse the processes of 1° and 2°. This work may be facilitated by placing any given configuration arrived at in 3° in any convenient position with reference to the axes of coordinates X, Y, Z, since such a shifting of the figure is equivalent to a change of variables (x_1, x_2) in the respective group G.

Beginning then with the simplest case where there is a single axis of rotation, we let this be the $X-$axis. Then $\sin 2v = 0$ and $\cos 2v = 1$. Hence S has the canonical form $(a, \bar{a})$; $a\bar{a} = 1$.

(A) G': a single axis of period g;

G: an abelian group (intransitive) of order g:

$$S_m = (\alpha^m, \alpha^{-m}); \quad m = 1, 2, \ldots, g; \quad \alpha^g = 1.$$

We next have a group G' containing the axis of period g in (A), in addition to g axes of period 2 lying in the plane $X=0$. Let one of the latter be the $Z-$axis; we here have $\cos 2v=-1$, $\cos 2(u-w)=1$, and the corresponding transformation of G is found to be

$$W=\begin{bmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{bmatrix}.$$

(B) *Dihedral group.*

G': one axis of period g and g axes of period 2;

G: an imprimitive group of order $2g\phi$ consisting of the transformations

$$S_m=(\pm\alpha^m,\ \pm\alpha^{-m}),\ W_m=\begin{bmatrix} 0 & \pm\alpha^m \\ \mp\alpha^{-m} & 0 \end{bmatrix};$$

$$m=1,\ 2,\ \ldots,\ g;\ \alpha^g=1.$$

57. **The tetrahedron and octahedron.** We now examine the five ordinary regular solids. Of these, the hexahedron and octahedron furnish the same set of axes of rotation, as do also the dodecahedron and icosahedron. We therefore have only three cases to consider: the tetrahedron, octahedron, and icosahedron.

In the case of the tetrahedron we have four vertices and correspondingly four axes of rotation of period 3; besides, three axes of period 2, each passing through the middle points of a pair of opposite edges. The latter are mutually perpendicular and may be taken as the $X-$, $Y-$, and $Z-$axes. The corresponding transformations of G are then as follows:

$$W_1=(i,\ -i),\ W_2=\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},\quad W_3=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\qquad i=\sqrt{-1},$$

either directly or after multiplication by $E_1=(-1,\ -1)$. If the vertices are named a, b, c, d, the three rotations

permute them among themselves according to the substitutions

$$(ab)(cd),\ (ad)(bc),\ (ac)(bd).$$

The remaining rotations permute the vertices three at a time cyclically, as (abc), . . . The corresponding transformations of G may be determined analytically from the conditions that they are each of order 3 and transform the *collineations* corresponding to W_1, W_2, W_3 cyclically. Certain ambiguities arise from the fact that the similarity-transformation $E_1=(-1,\ -1)$ is present in the group. Thus, $S=(abc)$ may transform W_1 into W_2 or into W_2E_1, etc. There results four possible forms for S, all of which are present in G if one of them is. We shall choose the following form:

$$S=\begin{bmatrix} \dfrac{-1+i}{2} & \dfrac{-1+i}{2} \\ \dfrac{1+i}{2} & \dfrac{-1-i}{2} \end{bmatrix}.$$

(C) *Tetrahedral group.*

G′: generated by (abc) and $(ab)(cd)$;

G: a group (primitive; § 60) of order 12ϕ generated by the transformations W_1 and S above.

The rotations of the octahedron include those of the tetrahedron (abc) and $(ab)(cd)$ if here a, b, c, d represent each a pair of opposite faces. To the list of generating rotations we now add one, U say, having the same axis as W_1, but being of period 4: $(acbd)$, or $U^2=W_1$. The corresponding transformation is easily determined from this last equation. We find that it has the canonical form

$$U=\left(\frac{1+i}{\sqrt{2}},\ \frac{1-i}{\sqrt{2}}\right).$$

(D) *Octahedral group.*

G': generated by (abc) and $(acbd)$;

G: a group (primitive) of order 24ϕ, generated by S and U above.

58. **The icosahedron.** Counting the rotations of an icosahedron we find

1 axis of period 1 (the identity),
15 axes of period 2,
20 axes of period 3, and
24 axes of period 5,

making 60 in all, the order of G'.

A Sylow subgroup of order 4 (§ 36) must be represented by three mutually perpendicular axes of period 2 (§ 55); moreover, two distinct subgroups of order 4 can have no axis of period 2 in common, since otherwise such an axis would be of higher period. Hence, the 15 axes of period 2 must belong to 5 subgroups of order 4.

It is readily observed that no rotation of G' can transform each of these subgroups into itself. It follows that G' can be written as a substitution group on 5 letters a, b, c, d, e, simply isomorphic with G' (§ 46). The 20 rotations of period 3 are represented by all the cycles on three letters; that is, the substitution group in question is the alternating group on 5 letters (§ 49).

Now, this group is generated by the following operators (§ 50): F_1, F_2, F_3 (corresponding to the substitutions (abc), $(ab)(cd)$, $(ab)(de)$), which satisfy the relations

$$F_1^3 = F_2^2 = F_3^2 = (F_1F_2)^3 = (F_2F_3)^3 = (F_1F_3)^2 = E.$$

For the corresponding transformations of G, we may evidently take respectively S, W_1 above, and a new transformation V which fulfils the conditions

$$V^2 = E \text{ or } E_1, \quad (W_1V)^3 = E \text{ or } E_1, \quad (SV)^2 = E \text{ or } E_1.$$

The first and last ambiguities fall away, since of necessity $V^2=(SV)^2=E_1$ (cf. § 51, 3°); and by using VE_1 if necessary instead of V we may take $(W_1V)^3=E$. We then find

$$V=\begin{bmatrix} \frac{i}{2} & \beta-i\gamma \\ -\beta-i\gamma & -\frac{i}{2} \end{bmatrix},$$

where

$$\beta=\frac{1-\sqrt{5}}{4}, \quad \gamma=\frac{1+\sqrt{5}}{4}.$$

(E) *Icosahedral group.*

G′: generated by certain rotations of periods 3, 2, 2, corresponding to the substitutions (abc), $(ab)(cd)$, $(ab)(de)$;

G: a group (primitive) of order 60ϕ generated by S, W_1, and V above.

The group (E) may be given the following useful form. Corresponding to the substitutions $S'=(abcde)$, $U'=(ad)(bc)$, $T'=(ab)(cd)$ of the alternating group on five letters, a set of generators

$$S'=(\epsilon^3, \epsilon^2),\ \epsilon^5=1;\ U'=\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix};\ T'=\begin{bmatrix} p & q \\ q & -p \end{bmatrix},\ p=\frac{\epsilon^4-\epsilon}{\sqrt{5}},\ q=\frac{\epsilon^2-\epsilon^3}{\sqrt{5}}$$

are constructed from the relations $S'^5=E$, $U'^{-1}S'U'=S'^{-1}$, $T'^2=E_1$, $U'^{-1}T'U'=T'$ or $=T'E_1$. The transformation S' is at the outset written in canonical form; during the subsequent determinations of U' and T' we simplify undetermined coefficients as much as possible by suitable changes of variables. The two types of groups (E) here given are equivalent (§ 51).

59. **Jordan's process.*** We shall in conclusion give an outline of Jordan's method for determining the linear groups in two variables.

* Jordan, *op. cit.*, in footnote to § 52; Valentiner, *op. cit.*, in the same footnote.

1°. It can be proved without difficulty that if two different abelian groups in two variables have in common a transformation S which is neither E nor E_1, then the transformations of the two groups are mutually commutative, so that they both belong to a single abelian group. (Writing S in canonical form, we find that a transformation which is commutative with it has the canonical form also.)

2°. Let K_1 be an abelian group written in canonical form. Then if T transforms K_1 into itself ($T^{-1}K_1T=K_1$; cf. § 30) and is not commutative with each of the transformations of K_1, we can readily prove that it must interchange the variables of K_1 (i.e., T has the form $\begin{bmatrix} 0 & a \\ b & 0 \end{bmatrix}$.

3°. Now let G be a linear group in two variables and of order $g\phi$. By 1°, we can sort its transformations into distinct abelian subgroups $K_1, K_2, \ldots, K_m$, of orders $k_1\phi, k_2\phi, \ldots, k_m\phi$, such that no transformation, except E and E_1, occurs in two distinct subgroups. Hence we have $g\phi=\phi+(k_1-1)\phi+(k_2-1)\phi+\ \ldots\ +(k_m-1)\phi$. (It is observed that E and E_1 are counted once each in the term ϕ in the right-hand member, but not in any of the numbers $(k_1-1)\phi, \ldots$.)

4°. The various groups $K_1, K_2, \ldots, K_m$ may be distributed into conjugate sets. Thus, if $K_1, K_2, \ldots, K_k$ make up one such set, the orders $k_1\phi, k_2\phi, \ldots$ are equal, and the subgroup H' which contains K_1 invariantively (cf. § 30) is, by 2°, of order $2k_1\phi$ or $k_1\phi$, according as there is, or is not, a transformation of type T in G interchanging the variables of K_1. Hence, if the subgroups are arranged in conjugate sets as suggested above, we get

$$g\phi=\phi+\frac{g\phi}{k_1}(k_1-1)+\ \ldots\ +\frac{g\phi}{2k_f}(k_f-1)+\ \ldots,$$

which reduces to

$$1=\frac{1}{g}+\sum\frac{k'-1}{k'}+\sum\frac{k''-1}{2k''}\,. \tag{1}$$

This *diophantine equation* is now shown to have a finite number of solutions for the integers $g, k', k'', \ldots$, and by the aid of these solutions the various groups G may be determined without much trouble.

Exercises

1. Construct the linear transformations in the variables X, Y, Z (cf. § 54) corresponding to the generating rotations W_1, W_2, W_3, S, U and V, §§ 57–58.

Hence show that the groups (C) and (D) have the monomial form (§ 60) when written in the variables X, Y, Z.

2. Verify the diophantine equation (1) for the groups (A) to (E). (Hint: to each abelian subgroup of G corresponds a single axis of rotation of G'.)

CHAPTER IV

ADVANCED THEORY OF LINEAR GROUPS*

A. ON IMPRIMITIVE GROUPS AND SYLOW SUBGROUPS

60. **Primitive and imprimitive groups.** Let us suppose that a group G contains not only transformations of the type given in the example in § 14, but also some of type

$$= \begin{bmatrix} p & q & t & v \\ -q & -p & -v & -t \\ u & w & r & s \\ -w & -u & -s & -r \end{bmatrix},$$

which upon the change of variables employed in § 14 becomes

$$\begin{bmatrix} 0 & 0 & p-q & t-v \\ 0 & 0 & u-w & r-s \\ p+q & t+v & 0 & 0 \\ u+w & r+s & 0 & 0 \end{bmatrix},$$

then we say that G is *imprimitive,* under the assumption that it is transitive.

In general, *a transitive group G, in which the variables* (either directly or after a suitable choice of new variables) *can be separated into two or more sets $Y_1, \ldots, Y_k$, such that the variables of each set are transformed into linear functions of the variables of the same set or into linear functions of the variables of a different set, is said to be imprimitive.* If such a division is not possible, the group

* We observe the rules laid down in § 51, with the exception that the transformations discussed in §§ 60–62 are not restricted to be of determinant unity.

is *primitive.* The sets $Y_1, \ldots, Y_k$ are called *sets of imprimitivity.*

THEOREM 1. *The n variables of an imprimitive linear group G may be so chosen that they break up into a certain number of sets of imprimitivity $Y_1, Y_2, \ldots, Y_k$ of m variables each ($n=km$), permuted among themselves according to a transitive substitution group* (§ 44) *K on the k letters $Y_1, \ldots, Y_k$, isomorphic with G. To the subgroup of K which leaves the letter Y_1 unaltered* (§ 45) *there corresponds a subgroup of G which is primitive as far as the variables of the set Y_1 are concerned.*

If $m=1$, $k=n$, then G is said to have the *monomial form* or to be a *monomial group.*

Proof.—The transformations $S_1, S_2, \ldots, S_h$ in G which transform the variables of each set into linear functions of the variables of that same set (there is at least one such transformation, namely E), form a group; moreover, if V is any transformation in G which permutes the sets in a certain way, then $S_1V, \ldots, S_hV$, and no others, permute them in the same way. If we therefore associate with each such system of h transformations a substitution on the letters $Y_1, \ldots, Y_k$, indicating the manner in which V permutes the corresponding sets of imprimitivity, we obtain a substitution group K, to which G is $(h, 1)$ isomorphic (§ 32).

Since G is a transitive linear group (§ 14), K must be a transitive substitution group (§ 44). Hence, K contains $k-1$ substitutions $T_2, T_3, \ldots, T_k$ which replace Y_1 by $Y_2, Y_3, \ldots, Y_k$ respectively (§ 45). Let us select $k-1$ corresponding transformations of G and denote them by $V_2, V_3, \ldots, V_k$. The conditions that their determinants must not vanish is found to imply that the sets contain an equal number of variables, say m, so that $n=km$. (A simple example will suffice to show this clearly, say $n=4$, $k=2$.)

There is in K a subgroup K_1 whose substitutions leave Y_1 unaltered (§ 45). This subgroup, together with the $k-1$ substitutions corresponding to $V_2, \ldots, V_k$ will generate K. Correspondingly, G is generated by $V_2, \ldots, V_k$ and that subgroup G_1 whose transformations replace the m variables of the set Y_1 by linear functions of the same variables, however they may permute the remaining sets. Let us fix our attention upon just that portion of each of the transformations of G_1 which affect only these m variables, and which may be looked upon as forming the transformations of a linear group $[G_1]$. We shall proceed to prove that *if* $[G_1]$ *is not primitive, then the variables in* G *may be changed in such a way that the number of new sets of imprimitivity is greater than* k.

Assuming then that $[G_1]$ is not primitive, its m variables are found to break up into at least two subsets of intransitivity or imprimitivity (either directly or after a change of variables). For the sake of definiteness we shall assume just two such sets, Y_1', Y_1''. New variables will now be introduced within the sets $Y_2, \ldots, Y_k$ such that V_2 will replace Y_1', Y_1'' by two distinct sets Y_2', Y_2'' in Y_2; and so on for each of the transformations $V_3, V_4, \ldots, V_k$. Let us temporarily write $(Y_r)T = Y_s$ to represent the phrase "T transforms the variables of the set Y_r into linear functions of the variables of the set Y_s"; and $(Y_r', Y_r'')T = (Y_s', Y_s'')$ to represent the phrase "T transforms the variables of any subset of Y_r into linear functions of the variables of a subset of Y_s" (that is, either $(Y_r')T = Y_s'$, $(Y_r'')T = Y_s''$; or $(Y_r')T = Y_s''$, $(Y_r'')T = Y_s'$). Then the properties of the $2k$ subsets relative to the transformations $V_2, \ldots, V_k$ may be stated in the form: $(Y_1', Y_1'')V_t = (Y_t', Y_t'')$, or its equivalent form: $(Y_t', Y_t'')\,V_t^{-1} = (Y_1', Y_1'')$; $t = 2, \ldots, k$.

It remains for us to prove that *any transformation* W *in* G *will permute these subsets among themselves;* that is,

assuming $(Y_p)W = Y_q$, then we have also $(Y'_p, Y''_p)W = (Y'_q, Y''_q)$. To show this, consider the transformation

$$T = V_p W V_q^{-1}.$$

This transformation belongs to G_1, since it transforms the set Y_1 into itself:

$$(Y_1)T = (Y_1)V_p W V_q^{-1} = (Y_p)W V_q^{-1} = (Y_q)V_q^{-1} = Y_1.$$

Hence, by assumption, $(Y'_1, Y''_1)T = (Y'_1, Y''_2)$; and, since $V_p W = T V_q$, so that $(Y'_1, Y''_1)V_p W = (Y'_1, Y''_1)T V_q$, we derive $(Y'_p, Y''_p)W = (Y'_q, Y''_q)$, what we set out to prove.

Accordingly, if $[G_1]$ is not primitive, we can change the n variables of G so as to increase the number of sets. This process may be continued until the sets contain just one variable each, or until we get a group $[G_1]$ which is primitive. Hence the theorem.

EXERCISES

1. Prove that there is only one type of imprimitive groups in three variables, namely the monomial type. Prove also that there is a single non-monomial type of imprimitive groups in four variables.

2. Prove that the group generated by $S = (-1, 1, -1)$ and T: $x_1 = -i(x'_1 + 2x'_2 + x'_3)/2$, $x_2 = (-x'_1 + x'_3)/2$, $x_3 = i(x'_1 - 2x'_2 + x'_3)/2$, is imprimitive. (Hint: By Exercise 1, the group must be monomial. Hence, if the new variables are x, y, z, the function xyz is a relative invariant (§ 88) of both S and T.)

61. Sylow subgroups.

LEMMA. *A linear group G which contains an invariant abelian subgroup H not composed entirely of similarity-transformations, is either intransitive or imprimitive.*

Proof.—Write H in canonical form. The variables can then be arranged in sets $X_1, X_2, \ldots$, having the property that a transformation of H affects all the variables of any one set by the same constant factor.

To illustrate, let H be generated by the transformations

$$T_1 = (\alpha_1, \alpha_1, \alpha_1, \alpha_1, \alpha_2) \qquad (\alpha_1 \neq \alpha_2),$$
$$T_2 = (\beta_1, \beta_1, \beta_2, \beta_2, \beta_2) \qquad (\beta_1 \neq \beta_2).$$

Here we have three sets: $X_1 = (x_1, x_2)$, $X_2 = (x_3, x_4)$, $X_3 = (x_5)$.

We shall for the moment write the phrase "T transforms the variables of the set X_p into one and the same constant multiple of themselves" symbolically: $(X_p)T = c(X_p)$. Thus, in the illustration given, $(X_2)T_2 = c(X_2)$, the constant multiple being β_2. More generally, if X' denotes an aggregate of certain linear functions $y_1, y_2, \ldots$ of the variables of the group, the equation $(X')T = c(X')$ implies that $(y_1)T = ay_1$, $(y_2)T = ay_2, \ldots, a$ being a constant, the same for every function $y_1, y_2, \ldots$ Then if $(X')T = c(X')$ for every transformation T of H, it follows that X' cannot contain variables from two or more distinct sets $X_1, X_2, \ldots$ For, otherwise at least one transformation in H would affect some of the letters involved by one constant factor, and others by a different constant factor.

Now let S and T be any transformations from G and H respectively. The variables of a given set X_p are by S transformed into linear functions of the variables of G, forming an aggregate which we shall denote by X'. Since H is invariant under G, the transformation $V = STS^{-1}$ belongs to H, and we have $(X_p)V = c(X_p)$. Hence,

$$(X_p)ST = (X_p)VS, \text{ or } (X')T = c(X').$$

Accordingly, the linear functions of X' must contain variables from only one set of H; in other words, S transforms the variables involved in X_p into linear functions of the variables of some one set of H. The sets $X_1, X_2, \ldots$ are therefore permuted among themselves by S, and the lemma is established.

THEOREM 2. *A linear group whose order is the power of a prime number can be written as a monomial group by a suitable choice of variables $x_1, x_2, \ldots, x_n$; that is, its transformations have the form:**

$$x_s = a_{st}x_t',$$

* First given by the author in *Transactions of the American Mathematical Society*, V (1904), 313–14; VI (1905), 232; see also Burnside, *Theory of Groups of Finite Order*, 2d ed., Cambridge, 1911, p. 352.

where s and t run through the numbers 1, 2, . . . , *n, though not necessarily in the same order.*

Proof.—1°. A group P whose order is the power of a prime number p is either abelian or it contains an invariant abelian subgroup Q whose transformations are not separately invariant under P (§ 35). In the first case the theorem follows from Theorem 10, § 22. In the second case, Q can be written in canonical form, and P is intransitive or imprimitive by the above lemma. If the theorem is true for a transitive group, it is evidently true for an intransitive group; hence we need merely consider the case where P is imprimitive.

2°. By Theorem 1, § 60, P is monomial unless there is a group $[P_1]$ which is primitive in the m variables of a set Y_1. But the latter alternative is impossible by 1°, since the order of $[P_1]$ is again a power of p, being a factor of such a number. Hence the theorem.

COROLLARY. *A linear group P in n variables, whose order is a power of a prime number p which is greater than n, is abelian.*

Proof.—Write P in monomial form. Then any transformation T which does not have the canonical form will permute the variables $x_1, x_2, \ldots, x_n$ in a certain manner, indicated by a substitution S on these letters. If the order of S is k, that of T is k or a multiple of k. Now, the order of T is a power of p (§ 28, Corollary); it follows that k is a power of p. But this is impossible since k is n or a product of numbers all less than n (cf. Exercise 4, § 41), and none of the prime factors involved can be p. Hence, every transformation of P has the canonical form, and this group is accordingly abelian.

EXERCISE

If p^b is the highest power of p which divides $n!$, prove that a Sylow subgroup of order p^a in n variables contains an invariant abelian subgroup of order p^{a-b} at least, if $a>b$.

62. **Theorem 3.** *A linear group in n variables and of order $g = g' p^a q^b r^c \ldots$, where $p, q, r, \ldots$ are different primes all greater than $n+1$, contains an abelian subgroup of order $p^a q^b r^c \ldots$.*

To prove this theorem by complete induction, we assume it true for any group in less than n variables and for any group in n variables whose order is less than g. That the theorem is then true for an intransitive group in n variables will be shown below (1°). There is left the case of a transitive group G of order g in n variables. It may be assumed that the determinants of the transformations of G are all unity (cf. 2° below).

At the outset we anticipate a theorem given later (cf. Exercise 2, § 90). From this it follows that G contains an abelian subgroup H_1 of order pq. This subgroup contains a transformation S of order p which is also contained in a Sylow subgroup P of G of order p^a (§ 39). The groups H_1 and P being abelian, S is invariant under both, and will therefore also be invariant under the group K generated by H_1 and P, whose order is divisible by $p^a q$. Now, S cannot be a similarity-transformation (by 2°; otherwise its determinant could not be unity); it follows that K is intransitive (cf. proof of Theorem 10, § 22), and must therefore, by 1°, contain an abelian subgroup H_2 of order $p^a q$.

Again, this subgroup H_2 and a certain Sylow subgroup Q of G of order q^b have in common a transformation T of order q, which must be invariant under both. We find, by the process above, an abelian subgroup H' of order $p^a q^b$. In the same way we obtain abelian subgroups $H'', \ldots$ of orders $p^a r^c, \ldots$.

Now, the subgroups of order p^a form a single conjugate set within G. We may therefore select such conjugates of $H'', H''', \ldots$, that these conjugates have in common with H' the group P. The group generated by them will be intransitive, the operators of P being invariant, and

its order will be a multiple of $p^a q^b r^c \ . \ . \ .$ The theorem follows by 1°.

1°. Consider an intransitive group G in two sets of intransitivity, the corresponding component groups being designated G' and G''. In G' we find, by assumption, an abelian subgroup K' of order $k' = p^\alpha q^\beta r^\gamma \ . \ .$, which we shall write in canonical form. Let the identity in G' correspond to a group G_1'' in G'', of order g_1''; the order of G will be the product of the orders of G' and G_1'' (§ 32). Now, in G_1'' we find an abelian subgroup K'' of order $p^\lambda q^\kappa r^\mu \ . \ .$; writing this in canonical form we see that the group generated by K' and K'' is the group sought.

2°. If the determinants of the transformations of G are not all unity, we construct a group G_1 by the method of § 12 whose transformations have this property. If then we find in G_1 an abelian group of order $p^\alpha q^\beta r^\gamma \ . \ .$, we evidently have a corresponding group in G, also abelian. The latter may contain similarity-transformations whose orders are prime to $p^a q^b r^c \ . \ .$; but these transformations can easily be disposed of (§ 34).

Exercises

1. If $n+1$ is a prime, and if the order of G is $g = g'(n+1)^t p^a q^b \ . \ .$, where $t>1$, and p, q, . . are primes greater than $n+1$, prove that there is in G an abelian subgroup of order $(n+1)^t p^a q^b \ . \ . \ .$

2. It follows from Theorem 3 that a group in n variables whose order is not divisible by a prime factor smaller than $n+2$ is abelian. Prove that if the order is not divisible by a prime factor smaller than $n+1$, the group is abelian.

B. ON THE ORDER OF PRIMITIVE GROUPS

63. The remainder of this chapter will be devoted to the discovery of limits to the magnitude of the prime factors that may enter the orders of primitive groups (§§ 63–64), to the highest admissible powers of the prime factors under certain conditions (§§ 65–68), and to the orders of abelian subgroups in general (§§ 69–73). The chapter closes with a discussion of the order of a primitive group (§ 74).

Theorem 4. *No prime number $p>7$ can divide the order of a primitive group G in three variables.*

The method of proof consists in showing that if the order g contains a prime factor $p>7$, then G is not primitive. We subdivide this process into four parts as follows: 1° proving the existence of an equation $F=0$, where F is a certain sum of roots of unity; 2° giving a method for transforming such an equation into a congruence (mod p); 3° applying this method to the equation $F=0$; 4° deriving an abelian self-conjugate subgroup P of order p^k.

1°. The order g being divisible by p, G contains a Sylow subgroup of order p^a and therefore a transformation S of order p. We choose such variables that S has the canonical form

$$S=(\alpha_1, \alpha_2, \alpha_3); \quad \alpha_1^p=\alpha_2^p=\alpha_3^p=1, \quad \alpha_1\alpha_2\alpha_3=1.$$

Two cases arise: two of the multipliers are equal, say $\alpha_1=\alpha_2$, or they are all distinct. They cannot all be equal, since $\alpha_1^3=1$ and $\alpha_1^p=1$ imply $\alpha_1=1$; whereas S is not the identity. Of the two cases we shall treat the latter only; the method would be the same in the former case,* and the result as stated in Theorem 4 would be the same.

Selecting from G any transformation V of order p:

$$V=\begin{bmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{bmatrix},$$

we form the products VS, VS^2, VS^μ. Their *characteristics* (§ 23) and that of V will be denoted by $[VS]$, . . . , $[V]$, and we have

$$\begin{aligned} [V] &= a_1 + b_2 + c_3, \\ [VS] &= a_1\alpha_1 + b_2\alpha_2 + c_3\alpha_3, \\ [VS^2] &= a_1\alpha_1^2 + b_2\alpha_2^2 + c_3\alpha_3^2, \\ [VS^\mu] &= a_1\alpha_1^\mu + b_2\alpha_2^\mu + c_3\alpha_3^\mu. \end{aligned} \tag{1}$$

* The congruence (7) would here be of the first degree in μ.

We now eliminate a_1, b_2, c_3, from these equations, obtaining

$$(2) \qquad \begin{vmatrix} [V] & 1 & 1 & 1 \\ [VS] & a_1 & a_2 & a_3 \\ [VS^2] & a_1^2 & a_2^2 & a_3^2 \\ [VS^\mu] & a^\mu & a_2^\mu & a_3^\mu \end{vmatrix} = 0 .$$

Expansion and division by $(a_1-a_2)(a_2-a_3)(a_3-a_1)$ gives us

$$(3) \qquad [VS^\mu]+K[V]+L[VS]+M[VS^2]=0 ,$$

K, L, M being certain polynomials in a_1, a_2, a_3 (§ 132), with the general term of type $a_1^a a_2^b a_3^c$. Since a_1, a_2, a_3 are powers of a primitive pth root of unity a (§ 133), the quantities K, . . . are certain sums of powers of a. Moreover, the characteristics $[V]$, . . . are each the sum of three roots of unity (Exercise 8, § 6). If, therefore, the products in (3) were multiplied out, there would result an equation of the kind discussed in § 133, 6°. The various terms could therefore be rearranged in sets as explained in that paragraph, which gives us an equation of the form

$$(4) \quad \begin{array}{l} A(1+a+a^2+ \ . \ . \ . \ +a^{p-1})+B(1+\beta+\beta^2+ \ . \ . \ . \\ +\beta^{p-1})+C(1+\gamma+\gamma^2+ \ . \ . \ . \ +\gamma^{r-1})+ \ . \ . \ . =0, \end{array}$$

A, B, C, . . . being certain sums of roots of unity; a, β, γ, . . . primitive roots of the equations $x^p=1$, $x^q=1$, $x^r=1$, . . . respectively; and p, q, r, . . . different prime numbers.

The coefficients A, B, C, . . . may be put into certain standard forms. Thus, any root $\epsilon \neq 1$ occurring in any of these sums will be assumed to be resolved into factors of prime-power indices (§ 133, 4°): $\epsilon=\epsilon_p\epsilon_q\epsilon_r \ . \ . \ .$, the root ϵ_p being of index p^m, ϵ_q of index q^n, etc. Furthermore, within A any root ϵ_p will be assumed to be either unity or a root whose index is divisible by p^2. For, if

ϵ_p were of index p, say $\epsilon_p = \alpha^k$, we could put 1 in its place, since

$$\alpha^k(1+\alpha+\alpha^2+ \ . \ . \ . \ +\alpha^{p-1}) \equiv \alpha^k+\alpha^{k+1}+\alpha^{k+2}+ \ . \ . \ .$$
$$+\alpha^{k+p-1} = 1+\alpha+\alpha^2+ \ . \ . \ . +\alpha^{p-1}$$

by means of the relation $\alpha^p = 1$. Likewise we assume that any root ϵ_q within B is either equal to unity or is a root whose index is divisible by q^2; and so on.

To illustrate, take $p=2$, $q=3$, and let i be a root of index 4 ($i^2=-1$) and τ a root of index 9 ($\tau^3=\omega$, $\omega^3=1$). Then the standard form for the expression

$$(-i\omega-1)(1-1)+(\tau^2\omega-\omega^2+i)(1+\omega+\omega^2) \tag{5}$$

would be

$$(i^3\omega+1)(1-1)+(\tau^5-1+i)(1+\omega+\omega^2).$$

2°. We shall now make certain changes in the values of the roots in the equation (4). First we put 0 for every root ϵ_q, ϵ_r, . . . whose index is divisible by the square of a prime other than p^2 (as τ^5 in the example above), leaving undisturbed the roots whose indices are not divisible by such a square, as α, α^2, . . . , β, ... Although these changes will turn the quantities A, B, . . . into certain new sums A', B', ... , the equation (4) is still true, since the vanishing factors $1+\alpha+\alpha^2+$ . . . $+\alpha^{p-1}$, etc., have not been affected.

Next we put 0 in place of $q-2$ of the roots β, β^2, . . . , β^{q-1}, and -1 for the remaining root, thus changing $B'(1+\beta+\beta^2+ \ . \ . \ . \ +\beta^{q-1})$ into $B'(1+0+0+$ . . . $+(-1))$, so that this product still remains equal to zero. Similarly we put 0 in place of $r-2$ of the roots γ, γ^2, . . . , γ^{r-1}, and -1 for the remaining root, and so on. Proceeding thus, we shall ultimately change (4) into an equation of the form

$$A''(1+\alpha+\alpha^2+ \ . \ . \ . \ +\alpha^{p-1}) = 0 \, ,$$

where A'' contains roots of the form $\pm\epsilon_p$ only.

Finally, we put 1 in the place of every root α, α^2, . . . , α^{p-1}, as well as every root ϵ_p. The left-hand member may then no longer vanish, but will in any event become a multiple of p.

The final value of the expression (5) would be $(\omega+1)(1+1)=2$ or 0, according as ω is replaced by 0 or -1.

Notation 1.—Any expression N which is a sum of roots of unity changed in the manner described above, shall be denoted by N'_p.

3°. We shall now study the effect of these changes upon the left-hand member of (3). Each of the characteristics $[VS]$, . . . , $[VS^\mu]$, being the sum of three (unknown) roots of unity, will finally become one of the seven numbers 0, ± 1, ± 2, ± 3, whereas $[V]$, being the sum of three roots of index 1 or p (cf. 1°), will become 3. The left-hand member of (3) will thus take the form

$$[VS^\mu]'_p+3K'_p+L'_p[VS]'_p+M'_p[VS^2]'_p, \tag{6}$$

and this number is a multiple of p, by 2°.

The values K'_p, L'_p, M'_p may be obtained by treating them as indeterminates 0/0. Thus,

$$K=\frac{-1}{(a_1-a_2)(a_2-a_3)(a_3-a_1)}\begin{vmatrix} a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \\ a_1^\mu & a_2^\mu & a_3^\mu \end{vmatrix}, \quad K'_p=\frac{0}{0}.$$

We find (cf. § 132)

$K'_p=-\frac{1}{2}(\mu-1)(\mu-2)$, $L'_p=\mu(\mu-2)$, $M'_p=-\frac{1}{2}\mu(\mu-1)$, and if we substitute in (6) and multiply by $p-1$ we obtain the congruence

$$[VS^\mu]'_p\equiv s\mu^2+t\mu+v \pmod p, \tag{7}$$

s, t, v being certain integers, the same for all values of μ.

We finally substitute in succession $\mu=0$, 1, 2, . . . , $p-1$ in the right-hand member of (7). The remainders

(mod p; cf. § 129) should all lie between -3 and $+3$ inclusive, the interval of the values of $[VS^\mu]'_p$. Now, each of these seven remainders can correspond to only two different values of μ less than p, if s and t are not both $\equiv 0 \pmod p$ (§ 130). Hence, there will correspond to each of the seven remainders at most 14 different values of μ, so that p is not greater than 14 unless $s \equiv t \equiv 0$. Trying $p=13$ and $p=11$, choosing for s, t, v the different possible sets of numbers $<p$ (the problem can be simplified by special devices),* we find that in no case can the remainders all be contained in the set $0, \pm 1, \pm 2, \pm 3$, unless $s \equiv t \equiv 0$. Choosing therefore this alternative we get, if $p>7$,

$$[VS^\mu]'_p \equiv v \pmod p.$$

In particular,

$$[VS]'_p \equiv v \equiv [V]'_p = 3 \pmod p,$$

from which it follows that $[VS]'_p = 3$. Again, from this equation we deduce that the roots of $[VS]$ are of index 1 or p. For if the index of one of these roots were divisible by the square of a prime, or by a prime different from p, then the changes indicated in 2° could be made at the outset in such a way that 0 or -1 would take the place of this root. But then $[VS]'_p$ would be one of the numbers $0, \pm 1, \pm 2, -3$.

4°. Accordingly, the product VS of any two transformations both of order p is a transformation of order p or 1. The totality of such transformations in G, together with E, will therefore form a group P (§ 27). The order of this group must be a power of p since it

* Since $a\mu + b$ runs through the p values $0, 1, 2, \ldots, p-1 \pmod p$ when μ does, we may substitute this expression for μ in the right-hand member of (7) and select the constants a, b so that this member takes a simpler form. For instance, if $p=11$, the right-hand member of (7) may be reduced by this substitution to one of the forms $\pm\mu^2 + c$; μ; or c; according as $s \not\equiv 0$; $s \equiv 0$, $t \not\equiv 0$; $s \equiv t \equiv 0 \pmod p$. When $p=13$ we get the forms $\pm\mu^2 + c$, $\pm 2\mu^2 + c$; μ; c.

contains no transformation whose order differs from p or 1. Moreover, P is invariant under G, since an operator of order p is transformed into one of order p (Exercise 2, § 30). Hence, G has an invariant subgroup P of order p^k. But this subgroup is abelian (§ 61, Corollary), and therefore G is intransitive or imprimitive (Lemma, § 61).

64. **Case of n variables.** Applying the process indicated in the previous paragraph to a group G in n variables, we select any two transformations S, V, both of order p, and write S in canonical form

$$S=(\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n).$$

Assuming that the multipliers $\alpha_1, \ldots, \alpha_n$ are all distinct, we find the following congruence corresponding to (7)

$$(8) \qquad [VS^\mu]'_p \equiv s\mu^{n-1}+t\mu^{n-2}+ \ \ldots \pmod p.$$

There are at most $2n+1$ different values that $[VS^\mu]'_p$ can take, namely $0, \pm 1, \pm 2, \ldots, \pm n$; and each corresponds to at most $n-1$ of the p values of μ: $0, 1, 2, \ldots, p-1$, if the right-hand member is not merely a constant. It follows that at most $(2n+1)(n-1)$ of these p values of μ can satisfy the congruence (8). Accordingly, if $p>(2n+1)(n-1)$, the right-hand member of (8) must be merely a constant; and then

$$[VS^\mu]'_p \equiv [VS]'_p \equiv [V]'_p = n \pmod p,$$

from which we find $[VS]'_p = n$. Now we deduce, as in 4°, § 63, that the transformation VS is of order p or 1, and from this that G has an invariant abelian subgroup of order p^k and is therefore not primitive. Hence the

THEOREM 5. *The order of a primitive linear group in n variables is not divisible by a prime number which is greater than $(2n+1)(n-1)$.*

In the case $n=4$ this limit is 27. But we may try out the congruence (8) in detail for the primes $p=23$, 19, . . , with the result that the right-hand member must reduce to a constant when $p>13$. For $p=13$ or 11 the process fails, as congruences of the form (8) exist for these primes (for instance, when $p=13$, (8) is satisfied if the right-hand member is the function $2\mu^3$).

EXERCISES

1. No transformation of variety m (cf. § 65) and of order p, a prime greater than $(2n+1)(m-1)$, can belong to a primitive group.

2. No primitive group G can contain a transformation of order p^2, if the prime p is greater than n (§ 67, Corollary). Hence prove that G cannot contain a subgroup of order p^2, if $p \geqq (2n+1)(n-2)$ and >2.

65. **The variety of a linear transformation and of an abelian group.** If the number of distinct multipliers of a transformation written in canonical form is k, we say that the transformation is of *variety* k. Thus, the transformation $S=(1, -1, -1)$ is of variety 2. By an obvious extension to abelian groups written in canonical form we say that such a group is of *variety* k if its variables may be separated into k sets in the manner explained in § 61. The group H of the illustration in that paragraph is accordingly of variety 3.

Notation 2.—An expression N which is the sum of a certain number of roots of unity, in which every root ϵ_p is replaced by 1, but in which none of the other changes indicated in 2°, § 63, are carried out, will be denoted by N_p. If $N=0$, then $N_p \equiv 0 \pmod{p}$.

66. **Theorem 6.** *Let a group G contain a transformation S of variety k and order $p^a\phi$, where $a>1$ and $p_a \gtrless kp$; p being a prime number. Then there is an invariant subgroup H_p in G (not excluding the possibility $G=H_p$) which*

contains $S^{p^{a-1}}$. *Any transformation in* H_p, *say* T, *has the property expressed by the following congruence:*

$$[V]_p \equiv [VT]_p \pmod{p}, \tag{9}$$

where V *is any transformation of* G.

The proof follows the plan of the proof of Theorem 4, § 63. We write S in canonical form, and construct the products VS, VS^2, . . . , VS^{k-1}, VR; R denoting $S^{p^{a-1}}$. As in 1°, we obtain an equation corresponding to (3):

$$[VR]+K[V]+L[VS]+ \ . \ . \ . \ +X[VS^{k-1}]=0.$$

However, the changes indicated in 2° are not carried out except that 1 is put for every root ϵ_p whose index is a power of p (cf. Notation 2).

All the coefficients L, . . . , X become multiples of p by this change (§ 132), and we find $K_p \equiv -1 \pmod{p}$. Hence finally,

$$[VR]_p - [V]_p \equiv 0 \pmod{p}. \tag{10}$$

Now consider all the conjugates R_1, . . . , R_h to R within G. They generate an invariant subgroup H_p (Exercise 3, § 31), and they all have the property of R as expressed by (10), since they fulfil the conditions of the theorem (cf. § 86, 3°). Moreover, any transformation T in H_p satisfies the congruence (9), since such a transformation can be written as the product of powers of R_1, . . . , R_h. For instance, let $T=R_1R_2$. By (10), we have $[VR_1]_p \equiv [V]_p$, and $[(VR_1)R_2]_p \equiv [VR_1]_p \pmod{p}$. Hence,

$$[VT]_p = [VR_1R_2]_p \equiv [VR_1]_p \equiv [V]_p \pmod{p}.$$

67. On the form of the group H_p. Let T be any transformation of H_p. Then by (9),

$$[T]_p = [ET]_p \equiv [E]_p = n \pmod{p},$$

and therefore, since T^m belongs to H_p also,

$$[T^m]_p \equiv n \pmod{p}.$$

Now let the order (say t) of T be prime to p, and let us assume that a of the multipliers of T are equal to each other, then b of the remaining multipliers equal, and so on. That is,

$$[T] = a\alpha_1 + b\alpha_2 + \ldots = [T]_p, \qquad a + b + \ldots = n,$$

and

$$[T^m] = a\alpha_1^m + b\alpha_2^m + \ldots = [T^m]_p.$$

Then we have (§ 133, 2°, 5°)

$$\sum_{m=1}^{t} [T^m]\alpha_1^{-m} = at \equiv n \sum_{m=1}^{t} \alpha_1^{-m}$$

$= 0$ or $= nt$, according as $\alpha_1 \neq 1$ or $\alpha_1 = 1$. Hence, we must have correspondingly $a \equiv 0$ or $\equiv n \pmod{p}$. Like results hold for the other numbers $b, \ldots$

If $p > n$, the congruence $a \equiv 0 \pmod{p}$ is impossible unless $a = 0$. It follows that every root α_s is unity. In other words, H_p can in this case contain no transformation whose order is prime to p. The order of H_p is therefore a power of p, and G is not primitive (cf. § 61). Hence the

COROLLARY. *No primitive group in n variables can contain a transformation of order p^2, if p is a prime number greater than n.*

Remark.—The group H_p as defined above may very well coincide with G. However, it may be shown that if a primitive group G contains a group H_p, then the latter (or a modified form of it) does not make up the whole of G, and n must be divisible by p*.

EXERCISE

No primitive group in n variables can contain a transformation of order p^3, if p is a prime greater than $n/2$.

* *Transactions of the American Mathematical Society*, XII (1911), 39–41.

68. **Theorem 7.** *Let G contain two commutative transformations $S=(\alpha_1, \ldots, \alpha_n)$ and $T=(\beta_1, \ldots, \beta_n)$, satisfying the following conditions:*

(A) Their orders are respectively $m\phi$ and $p\phi$, p being a prime number which is not a factor of m;

(B) the variety k of S is equal to or less than m;

(C) whenever $\alpha_s=\alpha_t$, then shall $\beta_s=\beta_t$ (the converse is not implied).

Under these conditions G has an invariant subgroup H_p which contains the transformation T.

Proof.—Let $V=[a_{st}]$ be any transformation of G, and let the products VS, VS^2, . . . , VS^{k-1}, VT be constructed. Eliminating $a_{11}, a_{22}, \ldots, a_{nn}$ from the equations $V=a_{11}+a_{22}+$ . . (cf. (1), § 63), we obtain an equation corresponding to (2), with the elements $[V]$, $[VS]$, . . . , $[VS^{k-1}]$, $[VT]$ in the first column. We now write 1 for every root ϵ_p whose index is a power of p, before expanding the determinant. The following changes will take place: the elements in the first column $[V]$ . . become $[V]_p$ . . (cf. Notation 2, § 65), and the elements of the last row, excepting $[VT]_p$, all become unity. Subtracting finally the last row from the first and expanding, we get

$$([V]_p-[VT]_p)D\equiv 0 \pmod{p},$$

D being the product of the differences of the k distinct roots among $\alpha_1, \ldots, \alpha_n$.

Now, since S^m is the identity or a similarity-transformation, $\alpha_1^m= \ldots =\alpha_n^m$. Hence, there is a rationalizing factor of $\alpha_s-\alpha_t$ such that the product is m or a factor of m. (For, put $\alpha_t/\alpha_s=\theta$, say, a root of index m_1 (a factor of m), and we have (§ 133, 5°) $(1-\theta)$ . . $\cdot(1-\theta^{m_1-1})=m_1$*). The product in question

*The value of $\lim_{x=1} \frac{x^{m_1}-1}{x-1}$.

is therefore a number prime to p. It follows that the product of D and a certain rationalizing factor is an integer N, prime to p. The resulting congruence may now be multiplied by an integer N' such that $NN' \equiv 1 \pmod{p}$, § 131), and we obtain

$$[V]_p - [VT]_p \equiv 0 \pmod{p}.$$

Finally, the existence of an invariant subgroup H_p, containing T, is proved as in § 66.

Another useful theorem based on the same principle as the last two is the following: *If a primitive group G in n variables contains an abelian subgroup of order $p^a\phi$ and variety k, where p is a prime, and $a \geqq k$, then G contains an invariant subgroup H_p which does not make up the whole of G, and p must be a factor of n.* Cf. reference given in Remark, § 67.

Exercises

1. Prove that no primitive group in four variables can contain two commutative transformations as follows: one of order $p=5$, 7, 11, or 13; the other of order q, prime to p, and of variety 4.

2. Under what conditions may two commutative transformations of different prime orders p and q belong to a group which contains no invariant subgroups H_p or H_q?

3. Let a group G in four variables contain an abelian subgroup generated by the group E, $S_2=(1, 1, -1, -1)$, $S_3=(1, -1, -1, 1)$, $S_4=(1, -1, 1, -1)$, and the transformation $T=(1, 1, \omega, \omega^2)$, where $\omega^3=1$. Prove that G contains an invariant subgroup of order 3^k, involving T.

69. **Unit-circle.** In the complex plane, a root of unity $\alpha = x+iy = \cos\theta + i \sin\theta$ represents a point on the *unit-circle* $x^2+y^2=1$. Accordingly, the multipliers of a transformation $S=(\alpha_1, \alpha_2, \ldots, \alpha_n)$ will represent m points on the unit-circle if S is of variety m. Thus, the multipliers of $S=(i, -i)$ represent two such points, separated by an arc of 180°.

We find it convenient in this and the next few paragraphs to indicate the matrix of a transformation $S=[a_{st}]$ by its first row: $S=[a_{11}\ a_{12}\ .\ .\ .\ .\ a_{1n}]$.

LEMMA 1. *Let* $S=(\alpha_1, \ .\ .\ , \alpha_n)$ *be a transformation in canonical form, whose multipliers are distributed over an arc* A *of the unit-circle of less than 180°, and let* T *be a unitary transformation* (§ 19). *Then no element in the principal diagonal of the matrix of the transformation* $V=TST^{-1}$ *can vanish.*

Proof.—There being no loss of generality by limiting ourselves to the case of three variables, we put $T=[a_{11}\ a_{12}\ a_{13}]$. Then (§ 19) $T^{-1}=[\bar{a}_{11}\ \bar{a}_{21}\ \bar{a}_{31}]$, and we find $TST^{-1}=[b_{11}\ b_{12}\ b_{13}]$, where

$$b_{ss}=a_{s1}\bar{a}_{s1}\alpha_1+a_{s2}\bar{a}_{s2}\alpha_2+a_{s3}\bar{a}_{s3}\alpha_3 \qquad (s=1,\ 2,\ 3).$$

Denote the number $a_{st}\bar{a}_{st}$ (which is real and positive unless $a_{st}=0$) by p_t. Then

$$p_1+p_2+p_3=1, \quad b_{ss}=p_1\alpha_1+p_2\alpha_2+p_3\alpha_3.$$

Now, if we regard α_1, α_2, α_3 as unit vectors radiating from the center of the unit-circle to points of the arc A, the sum b_{ss} will evidently be a non-vanishing vector lying in the angle subtended by the arc A. Hence the lemma.

It is furthermore evident that the *length* of the vector b_{ss} is less than the sum of the lengths of the vectors $p_1\alpha_1$, $p_2\alpha_2$, $p_3\alpha_3$ (namely $p_1+p_2+p_3=1$), unless those of the vectors just mentioned which do not vanish have the same direction. Hence the

LEMMA 2. *No element* b_{ss} *of the matrix of* V *of Lemma 1 can be a root of unity* (*or even be of unit length*) *unless those of the vectors* $p_1\alpha_1, \ .\ .\ .\ , p_n\alpha_n$ *which do not vanish, have the same direction. Hence, if* b_{ss} *is a root of unity, and if neither* a_{st} *nor* a_{sv} *vanish, then* $\alpha_t=\alpha_v$.

70. **Theorem 8.** *If a group G contains a transformation $S=(\alpha_1, \ldots, \alpha_n)$ whose multipliers, when located on the unit-circle, occupy an arc $\leqq 120°$ and extending not more than $60°$ on either side of some one of them, say α_1,* then G is not primitive.* (It is assumed that S is not a similarity-transformation.)

Let $n=3$ to begin with. We assume that G has the unitary form and that at the same time S has the canonical form (Corollary, § 22). Furthermore, we assume for the present that

$$\alpha_1 \neq \alpha_2, \quad \alpha_1 \neq \alpha_3, \tag{11}$$

leaving to the end of § 71 the treatment of the general case.

We shall prove in order

(A) The transformation S and all its conjugates in G generate an intransitive group G' (§ 71).

(B) Due to the invariance of G' (Exercise 3, § 31), the group G cannot be primitive (§ 72).

71. *Proof of* (A).—Since the multipliers α_1, α_2, α_3 all lie on an arc$\leqq 120°$, no element in the principal diagonal of any conjugate of S can vanish (Lemma 1, § 69). Hence, if $V=[b_{11}\ b_{12}\ b_{13}]$ is such a conjugate, then $b_{11} \neq 0$. Now, if $b_{12}=b_{13}=0$ for every conjugate, the group G' generated by these conjugates is reducible and therefore intransitive (§ 20).

The proposition (A) is therefore established by proving $b_{12}=b_{13}=0$. To this purpose let us denote by M the aggregate of all those conjugates of S, if any, for which at least one of the two elements b_{12}, b_{13} does not vanish.

* For an illustration, take the transformation of order 6 in three variables whose multipliers are $\alpha_1=1$, $\alpha_2=-\omega$, $\alpha_3=-\omega^2$, where $\omega^3=1$; or one of order 7 whose multipliers are $\alpha_1=1$, $\alpha_2=\cos v+i\sin v$, $\alpha_3=\alpha_2^{-1}=\cos v-i\sin v$, where $v=(360/7)°$.

Let $T'=[a'_{11}\ a'_{12}\ a'_{13}]$ be any one of these. We then introduce a function $f(T')$ defined as follows:

$$f(T')=+\sqrt{a'_{11}\bar{a}'_{11}}\,.$$

We have

$$f(T')<1\,, \tag{12}$$

since $a'_{11}\,\bar{a}'_{11}+a'_{12}\,\bar{a}'_{12}+a'_{13}\,\bar{a}'_{13}=1$ (if $a'_{11}\,a'_{11}=1$, it would of necessity follow that $a'_{12}=a'_{13}=0$, contrary to the hypothesis concerning M).

We now let $T=[a_{st}]$ be that transformation in the aggregate M for which $f(T)$ has the greatest value. Constructing $T_1=TST^{-1}$ we shall then demonstrate the following properties of T_1:

(1°) $f(T_1)>f(T)$,* (2°) T_1 belongs to M,

thus violating the assumption as to T. *The conclusion is drawn that M does not exist.*

To prove (1°), put $a_2/a_1=\cos v_2+i\,\sin v_2$, $a_3/a_1=\cos v_3+i\,\sin v_3$, and we find

$$f(T_1)=\sqrt{(A+iB)(A-iB)}=\sqrt{A^2+B^2}\geqq A\,,$$

where

$$A=a_{11}\bar{a}_{11}+a_{12}\bar{a}_{12}\cos v_2+a_{13}\bar{a}_{13}\cos v_3\,.$$

Now, by the condition of the theorem,

$$-60°\leqq v_s\leqq+60°\ (s=2,\ 3),\ \text{so that}\ \cos v_s\geqq\tfrac{1}{2}\,.$$

* The use of an inequality of this kind is in substance a discovery of Valentiner's (*De endelige Transformations-Gruppers Theori*, Copenhagen, 1889, p. 115). An equivalent inequality is used in an ingenious manner by Bieberbach to find a limit to the orders of linear groups. (See *Sitzungsberichte der Kgl. Preussischen Akademie der Wissenschaften*, 1911, pp. 231–40; also two papers by Frobenius in the same *Proceedings* (1911) pp. 241–48 and pp. 373–78.

Hence, we derive

$$f(T_1) \geqq A \geqq a_{11}\bar{a}_{11} + \tfrac{1}{2}(a_{12}\bar{a}_{12} + a_{13}\bar{a}_{13}) = a_{11}\bar{a}_{11} + \tfrac{1}{2}(1 - a_{11}\bar{a}_{11})$$
$$= \tfrac{1}{2}(1 + a_{11}\bar{a}_{11}) = \tfrac{1}{2}(1 + \{f(T)\}^2) .$$

Accordingly, since $1+\lambda^2 > 2\lambda$ unless $\lambda = 1$, and $f(T) \neq 1$ by (12), it follows that

$$f(T_1) \geqq \tfrac{1}{2}(1 + \{f(T)\}^2) > f(T) .$$

To prove (2°), we first notice that $T_1 = TST^{-1}$ is a conjugate of S. It remains for us to show that, if $T_1 = [b_{11}\ b_{12}\ b_{13}]$, b_{12} and b_{13} do not both vanish.

Assume the contrary: $b_{12} = b_{13} = 0$. Then $b_{11}\bar{b}_{11} = 1$, so that the *vector* b_{11} is of unit length (in fact, b_{11} must be a root of unity). But,

$$b_{11} = a_{11}\bar{a}_{11}a_1 + a_{12}\bar{a}_{12}a_2 + a_{13}\bar{a}_{13}a_3 ,$$

and therefore, since $a_{11} \neq 0$ (Lemma 1, § 69), and since by assumption either a_{12} or $a_{13} \neq 0$, say $a_{12} \neq 0$, we have $a_1 = a_2$ (Lemma 2, § 69), contrary to the hypothesis (11). Hence T_1 belongs to M if T does.

In the general case, the multipliers of S may be repeated. Assume that $a_1, a_2 \ldots$ occur respectively $m, k, \ldots,$ times:

$$S = (a_1, \ldots, a_1;\ a_2, \ldots, a_2;\ \ldots) .$$

The aggregate M consists here of all those conjugates $V = [b_{st}]$ of S for which the equations

$$(13) \quad b_{st} = 0 \quad (s = 1, 2, \ldots, m;\ t = m+1, m+2, \ldots, n)$$

are not *all* satisfied: As above, the proof of (A) depends on showing that such an aggregate does not exist; and to this end the function $f(T')$ is introduced, which now has the form

$$f(T') = +\sqrt{(a'_{11} + a'_{22} + \ldots + a'_{mm})(\bar{a}'_{11} + \bar{a}'_{22} + \ldots + \bar{a}'_{mm})} .$$

In place of (12) we here have $f(T') < m$. The inequality (1°) $f(T_1) > f(T)$ is proved without difficulty.

To prove (2°) we assume first that $T_1 = TST^{-1}$ does *not* belong to M; that is, if $T_1 = [b_{st}]$, we assume the set (13) *true*. Now we write T_1 in canonical form as far as the first m variables are concerned; S will still have the canonical form, and G can still be written as a unitary group. Moreover, the new aggregate M will coincide with the old. If then $T_1 = (\theta_1, \theta_2, \ldots, \theta_m)$ as far as the first m variables are concerned, we have

$$\begin{aligned}\theta_1 = (a_{11}\bar{a}_{11} + \ldots + a_{1m}\bar{a}_{1m})\alpha_1 + (a_{1\,m+1}\bar{a}_{1\,m+1} + \ldots \\ + a_{1\,m+k}\bar{a}_{1\,m+k})\alpha_2 + \ldots,\end{aligned}$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\begin{aligned}\theta_m = (a_{m1}\bar{a}_{m1} + \ldots + a_{mm}\bar{a}_{mm})\alpha_1 + (a_{m\,m+1}\bar{a}_{m\,m+1} + \ldots \\ + a_{m\,m+k}\bar{a}'_{m\,m+k})\alpha_2 + \ldots\end{aligned}$$

By using the Lemma 2, § 69, and the facts that $T = [a_{st}]$ belongs to M and that none of the numbers $a_{11}, a_{22}, \ldots, a_{mm}$ vanish, we prove readily that at least one of the system of equations just written is impossible. Hence T_1 belongs to M.

72. *Proof of (B); general case.* By (*A*), the first m variables $x_1, \ldots, x_m$ are transformed into linear functions of themselves by S and its conjugates, if α_1 is repeated m times among the multipliers of S. The group G' generated by these conjugates is therefore reducible, and hence also intransitive; say in the two sets $X = (x_1, \ldots, x_m)$, $Y = (x_{m+1}, \ldots, x_n)$ to begin with.

Now let G' be broken up into its ultimate sets of intransitivity in any way whatsoever, without reference to the original intransitive set X. Then if $y_1, \ldots, y_k$ is a set of intransitivity, and if S is written in canonical form as far as this set is concerned, its multipliers within the set are all $= \alpha_1$, or none of them are. (That is, in the first case the variables are linear functions of $x_1, \ldots, x_m$; in the last case they are linear functions of $x_{m+1}, \ldots, x_n$.) This is easily seen when $y_1, \ldots, y_k$ are expressed as functions of $x_1, \ldots, x_n$, and the condition imposed that S transforms these functions into constant multiples of themselves. Thus, we find that if f multipliers are equal

to α_1, and the remaining multipliers are not, then f variables, say $y_1, \ldots, y_f$, are functions of $x_1, \ldots, x_m$ only, and the remaining variables $y_{f+1}, \ldots, y_k$ functions of $x_{m+1}, \ldots, x_n$ only. Since these two sets make up a single intransitive set for G', and the sets X, Y are separately intransitive sets, it follows that $(y_1, \ldots, y_f)$ and $(y_{f+1}, \ldots, y_k)$ must make up two intransitive sets.

What has just been said with regard to S will be true of any conjugate of S within G, since such a conjugate might have been chosen for S in the first place (conjugate transformations have the same multipliers; cf. Theorem 11, § 23). Hence, as now written, G' possesses the property that any one of the conjugates of S will appear partly in the canonical form, namely in regard to the m variables that correspond to its m multipliers α_1.

Now, a given set of intransitivity may have the property that several conjugates $S_1, \ldots, S_p$ have the canonical form $(\alpha_1, \ldots, \alpha_1)$ for this set. Calling p the "index" of the set in question, we seek the sets of highest index π. *Then we can show that G permutes these sets among themselves, thus proving (B).*

Let $(z_1, \ldots, z_h)$ be such a set, and let $S_1, \ldots, S_\pi$ be the corresponding conjugates. Selecting any transformation V in G, we write $V^{-1}S_1V = T_1, \ldots, V^{-1}S_\pi V = T_\pi$, and $(z_1)V = v_1, \ldots, (z_h)V = v_h$. Then we have

$$(z_1, \ldots, z_h)S_jV = (z_1, \ldots, z_h)VT_j \qquad (j = 1, 2, \ldots, \pi);$$

i.e.,

$$\alpha_1(v_1, \ldots, v_h) = (v_1, \ldots, v_h)T_j .$$

The variables $v_1, \ldots, v_h$ are therefore transformed into $\alpha_1 v_1, \ldots, \alpha_1 v_h$ by the maximum number of distinct conjugates, namely $T_1, \ldots, T_\pi$. It follows that $v_1, \ldots, v_h$ are linear functions of the variables of a *single* set of index π. For, it is easily seen that if a certain linear function

v of the variables of G is transformed into $\alpha_1 v$ by the *maximum* number of conjugates, v must, of necessity, be a linear function of the variables of some one of the sets of index π.

73. **Theorem 9.** *If a linear group G contains an abelian subgroup K of variety m (§ 65) and order $k\phi$, where $k \geqq 6^{m-1}-(6^{m-2}+6^{m-3}+ \ . \ . \ +6)$, then G is intransitive or imprimitive.*

We can prove that there is in K a transformation all of whose multipliers are not more than $\pm 60°$ removed from some one of them when plotted on the unit-circle. Theorem 8 may then be applied.

Let K be written in canonical form, and let the variables be arranged in m sets according to the method explained in § 61. The case $n=m=4$ will be discussed in detail; it will then be sufficiently obvious how to prove the theorem for the general case. Furthermore, since only the mutual ratios of the multipliers are of importance in Theorem 8, a slight simplification can be effected by adopting the form $S'=(1, \ \beta/\alpha, \ \gamma/\alpha, \ . \ . \ )$ instead of $S=(\alpha, \beta, \gamma, \ . \ . \ )$. Thereby we gain an additional advantage: the order of the group composed of the transformations S', . . is k when the order of the corresponding group S, . . is $k\phi$ (§ 51, 3°).

Accordingly, we have $k \geqq 6^3-(6^2+6)$ distinct transformations

$$(14) \qquad S_t=(1, \ \alpha_t, \ \beta_t, \ \gamma_t) \qquad (t=1, \ 2, \ . \ . \ , \ k) \ .$$

We now plot the points $\alpha_1, \ \alpha_2, \ . \ . \ , \ \alpha_k$ on the unit-circle. Starting at one of these points, we divide the circle into 6 equal parts. It is evident that one at least of these parts will contain more than $k/6$ points, either within or upon its boundary. (In the case under discussion, one part will contain at least 6^2-6 points.) There are

therefore 6^2-6 or more points which are not separated one from another by more than 60°. Let the corresponding transformations of the set (14) be denoted by S_1, S_2, . . , S_{30}.

We next plot the points $\beta_1, \beta_2, \ldots, \beta_{30}$ on the unit-circle. Dividing this circle as before, we find at least $30/6+1$ points lying on one of the arcs of 60°, corresponding to the transformations S_1, S_2, . . S_6. We finally plot the points $\gamma_1, \ldots, \gamma_6$ and find at least 2 points on an arc of 60°. If the corresponding transformations are S_1, S_2, it is plain that their corresponding multipliers are never more than 60° apart. It follows that the transformation $S_2S_1^{-1}=(1, \alpha_2/\alpha_1, \beta_2/\beta_1, \gamma_2/\gamma_1)$ fulfils the conditions imposed on S in Theorem 8, the root α_1 there being unity here.

NOTE.—By modifying to some extent the principle developed in §§ 69–72, and by using certain processes in the Geometry of Numbers (cf. *Transactions of the American Mathematical Society*, XV (1914), 227), the author has obtained a very much lower limit than the one given in Theorem 9; namely $k \leqq h^{m-1}$, where h is a number lying between 3 and 5, depending on the nature of the prime factors involved in the order of the group K. The proof of this result has not yet been published.

EXERCISES

1. In a group G, a transformation all of whose multipliers lie on an arc $<60°$ is commutative with one whose multipliers lie on an arc $<180°$ (Frobenius).

2. Prove that if a group G contains a transformation T all of whose multipliers lie on an arc $<72°$, then G is not primitive. (Hint: Either T or T^5 fulfils the conditions imposed on S of Theorem 8.)

3. By Theorem 9, a primitive group G cannot contain an abelian subgroup of variety 3, whose order $k\phi$ is equal to or greater than 30ϕ. Examine in detail the possibilities $k=26$, 27, 28, 29, and prove that $k<26$.

74. Order of a primitive group in n variables. We are now in a position to set a superior limit to the order $g\phi$

of a primitive group G in n variables. A Sylow subgroup of order p^a is monomial and must contain an abelian subgroup of order p^{a-b} at least, where p^b denotes the highest power of p which divides $n!$ (Exercise, § 61). Hence, by § 73, Note,

$$p^a \leqq p^b 5^{n-1}\phi ,$$

and that part of g which is made up of prime factors not greater than n is not greater than $n!5^{(n-1)\theta(n)}\phi$, where $\theta(n)$ denotes the number of primes smaller than $n+1$. Again, if $n+1$ is a prime and is a factor of g, the corresponding Sylow subgroup is abelian (Corollary, § 61) and its order is $\leqq 5^{n-1}$. Finally, the remaining factor of g is the order of an abelian group (§ 62) and is also $\leqq 5^{n-1}$. It follows that the order of a primitive group in n variables is

$$g\phi \leqq n!5^{(n-1)\theta(n)+2}\phi .$$

HISTORICAL NOTE.—In 1878 Jordan proved the classical theorem that the order of a finite linear group in n variables is of the form λf, where f is the order of an abelian self-conjugate subgroup, and where λ is inferior to a fixed number which depends only upon n.* Definite limits to λ have been given by Schur for the case where the characteristics belong to a given algebraic domain;† by Bieberbach and Frobenius‡ and by the author.§

Concerning the theorems of §§ 60–68, see *Transactions of the American Mathematical Society*, IV, 387–97; V, 310–20; VI, 230–32; VII, 523–29; XII, 39–42.

* *Journal für die reine und angewandte Mathematik*, Bd. 84, p. 91.

† *Sitzungsberichte der Königlich-Preussischen Akademie der Wissenschaften*, 1905, pp. 77 ff.

‡ *Sitzungsberichte*, etc., 1911, pp. 231 ff., 241 ff.

§ *Transactions of the American Mathematical Society*, V (1904), 320–21 for primitive groups; VI (1905), 232 for imprimitive groups.

CHAPTER V

THE LINEAR GROUPS IN THREE VARIABLES

75. **Introduction.** The determination of the linear groups in three variables is here based on the following classification:

1. Intransitive and imprimitive groups.
2. Primitive groups having invariant intransitive or imprimitive subgroups.
3. Primitive groups whose corresponding collineation groups are simple ("primitive simple groups").
4. Primitive groups having invariant primitive subgroups.

No specific theory is needed for the determination of the groups in the first class, beyond that given in § 60. For the determination of the groups in class 3 the theorems of §§ 61–73 are very useful.

The notation and conventions laid down in § 51 are observed throughout the chapter.

76. **Intransitive and imprimitive groups.** There are two types of *intransitive groups:*

(A) $x_1 = \alpha x_1',\ x_2 = \beta x_2',\ x_3 = \gamma x_3'$ (abelian type).
(B) $x_1 = \alpha x_1',\ x_2 = ax_2' + bx_3',\ x_3 = cx_2' + dx_3'$.

In (B) the variables x_2, x_3 are transformed by a linear group in two variables (cf. chap. iii).

The *imprimitive* groups are all monomial. There are two types:

(C) A group generated by an abelian group

$$H: \quad x_1 = \alpha x_1', \quad x_2 = \beta x_2', \quad x_3 = \gamma x_3'$$

and a transformation which permutes the variables in the order $(x_1 x_2 x_3)$. This transformation may be written in the form

$$T: \quad x_1 = x_2', \quad x_2 = x_3', \quad x_3 = x_1',$$

by a suitable choice of variables.

(D) A group generated by H, T of (C) and the transformation

$$R: \quad x_1 = a x_1', \quad x_2 = b x_3', \quad x_3 = c x_2'.$$

77. **Remarks on the invariants of the groups** (C) **and** (D). Interpreting x_1, x_2, x_3 as homogeneous co-ordinates of the plane, the triangle whose sides are $x_1 = 0$, $x_2 = 0$, $x_3 = 0$ is transformed into itself by the operators of (C) and (D); in other words, $x_1 x_2 x_3$ is an invariant of these groups.

Later on it becomes necessary for us to know under what conditions there are other invariant triangles. Assuming the existence of one such, say

$$(1) \qquad (a_1 x_1 + a_2 x_2 + a_3 x_3)(b_1 x_1 + b_2 x_2 + b_3 x_3)(c_1 x_1 + c_2 x_2 + c_3 x_3) = 0,$$

we operate successively by the transformations of H and by T. Observing that α, β, γ cannot all be equal for every transformation of H, as otherwise (C) and (D) would be intransitive, we find by examining the various possibilities that (1) could not be distinct from $x_1 x_2 x_3 = 0$ unless H is the particular group generated by the transformations

$$S_1 = (1, \omega, \omega^2), \quad S_2 = (\omega, \omega, \omega); \quad \omega^3 = 1.$$

There are then four invariant triangles for (C), namely:

$$x_1x_2x_3=0;$$
$$(2)\quad (x_1+x_2+\theta x_3)(x_1+\omega x_2+\omega^2\theta x_3)(x_1+\omega^2 x_2+\omega\theta x_3)=0$$
$$(\theta=1,\ \omega,\ \text{or}\ \omega^2)\,.$$

In the case of (D), these four triangles will be invariant if the group is generated by S_1, S_2, T and R, the latter now having the form

$$R:\ x_1=-x_1',\ \ x_2=-x_3',\ \ x_3=-x_2',$$

either directly or after multiplication by suitable powers of S_1 and S_2.

78. **Groups having invariant intransitive subgroups.** A group having an invariant subgroup of type (A) is intransitive or imprimitive (Lemma, § 61), and a group having an invariant subgroup of type (B) is intransitive. For, let V be any transformation of such a group, and T any transformation of (B). Then $VTV^{-1}=T_1$ belongs to (B), and if we put $(x_1)T_1=ax_1$, $(x_1)V=y$, we have

$$(y)T=(y)V^{-1}T_1V=(x_1)T_1V=a(x_1)V=ay\,.$$

This shows that $y=0$ is an invariant straight line for (B). But $x_1=0$ is the only such line, and therefore $y=(x_1)V=kx_1$, $k=$constant. The group in question is therefore reducible and hence intransitive.

79. **Primitive groups having invariant imprimitive subgroups.** We now consider a group G containing an invariant subgroup of type (C) or (D), § 76. These types leave invariant the triangle $x_1x_2x_3=0$ (§ 77), and if this is the only one, we could prove by the method of § 78 that G would also transform this triangle into itself. But then G would not be primitive. We therefore assume

that there are four invariant triangles for (C) and (D), permuted among themselves by the transformations of G. Let us denote the triangles by t_1, t_2, t_3, t_4, in order as they are listed in (2).

We now associate with each transformation in G a substitution on the letters t_1, t_2, t_3, t_4, indicating the manner in which the transformation permutes the corresponding triangles. We thus obtain a substitution group K on four letters to which G is multiply isomorphic (§ 32), and the invariant subgroup (C) or (D) corresponds to the identity of K. No one of the four letters could be left unchanged by every substitution of K. For the corresponding triangle would be invariant under G; and bringing this triangle into the form $x_1x_2x_3=0$ by a suitable choice of new variables, G would appear in intransitive or imprimitive form. Moreover, no transformation can interchange two of the triangles and leave the other two fixed, as may be verified directly.

Under these conditions we find the following possible forms for K:

(E′) 1, $(t_1t_2)(t_3t_4)$;*

(F′) 1, $(t_1t_2)(t_3t_4)$, $(t_1t_4)(t_2t_3)$, $(t_1t_3)(t_2t_4)$;

(G′) the alternating group on four letters, generated by $(t_1t_2)(t_3t_4)$ and $(t_2t_3t_4)$.

Now, to construct the corresponding linear transformations we observe first that the group (D) as given in § 77 contains all the transformations which leave invariant each of the four triangles. Next we note that if a given transformation V permutes the triangles in a certain manner, then any transformation V' which permutes them in the same manner can be written in the form $V'=XV$, X being a transformation of (D). For, $V'V^{-1}$ must leave

* The three types of G corresponding to the three substitution groups: E, $(t_1t_2)(t_3t_4)$; E, $(t_1t_3)(t_2t_4)$; E, $(t_1t_4)(t_2t_3)$ are *equivalent* (§ 51).

fixed each triangle, and is therefore a transformation X as defined.

We are now in a position to construct the required groups. By direct application we verify that the transformations U, V, UVU^{-1}:

$$
\begin{aligned}
&U\colon\ x_1=\epsilon x_1',\ x_2=\epsilon x_2',\ x_3=\epsilon\omega x_3' && (\epsilon^3=\omega^2);\\
&V\colon\ x_1=\rho(x_1'+x_2'+x_3'),\ x_2=\rho(x_1'+\omega x_2'+\omega^2 x_3'),\\
&\qquad x_3=\rho(x_1'+\omega^2 x_2'+\omega x_3') && \left(\rho=\frac{1}{\omega-\omega^2}\right);\\
&UVU^{-1}\colon\ x_1=\rho(x_1'+x_2'+\omega^2 x_3'),\ x_2=\rho(x_1'+\omega x_2'+\omega x_3'),\\
&\qquad x_3=\rho(\omega x_1'+x_2'+\omega x_3');
\end{aligned}
\tag{3}
$$

permute the triangles in the following manner:

$$(t_2t_3t_4),\quad (t_1t_2)(t_3t_4),\quad (t_1t_4)(t_2t_3).$$

Accordingly, since all the groups required contain a transformation corresponding to $(t_1t_2)(t_3t_4)$, every such group must contain a transformation XV, X belonging to (D). Hence, if G contains (D) as a subgroup, it also contains V. If, however, (C) were a subgroup of G, but not (D), then either V is contained in G, or else XV, where X is a transformation contained in (D) but not in (C). In this event X may be written X_1R, where X_1 belongs to (C). Hence, finally, either V or RV belongs to G. However, $V^2=(RV)^2=R$. Thus R, and therefore also V, are contained in G in any case.

Again, if G contains a transformation corresponding to $(t_2t_3t_4)$ or $(t_1t_4)(t_2t_3)$, such a transformation can be written XU or $XUVU^{-1}$, X belonging to (D). Hence, since G contains (D) as we have just seen, it will contain either U or UVU^{-1} in the cases considered. We therefore have the following types:

(E) Group of order 36ϕ generated by (C) as given in § 77:

$$S_1=(1,\ \omega,\ \omega^2),\quad T:\ x_1=x_2',\ x_2=x_3',\ x_3=x_1';$$

and the transformation V of (3).

(F) Group of order 72ϕ generated by S_1, T, V and UVU^{-1}.

(G) Group of order 216ϕ generated by S_1, T, V and U.

These groups are all primitive, and they all contain (D) as an invariant subgroup. The group (G) is called the *Hessian group.**

80. **Primitive simple groups:† the Sylow subgroups.** In order to utilize Theorems 4–7, chap. IV, it becomes necessary for us to study the effect of the presence in a group G of an invariant subgroup H_p; or, since G is here to be a simple group,‡ to determine the possibility $G=H_p$. Now, it is at once seen that no transformation $T=(\alpha_1,\ \alpha_2,\ \alpha_3)$ whose order is prime to p, can belong to H_p, by the results of § 67. Accordingly, the order of H_p is a power of p. However, a group of this order is not primitive (§ 61), and therefore we shall dismiss from consideration in §§ 80–81 all groups which may be shown to contain H_p, as for instance a group containing the transformation $T=(-1,\ i,\ i)$, where $i=\sqrt{-1}$ (cf. § 66), or the transformation $T=(\omega_1,\ \epsilon\omega_2,\ \epsilon^2\omega_3)$, where $\omega_1^3=\omega_2^3=\omega_3^3=1$, and where ϵ is a primitive 9th root of unity. On the other hand, the presence of the transformation $T=(\epsilon\omega_1,\ \epsilon\omega_2,\ \epsilon\omega_3)$ does not imply the presence of a subgroup H_p.

* Cf. Jordan, *Journal für die reine und angewandte Mathematik*, Bd. 84 (1878), p. 209.

† Such a group may contain the group of similarity-transformations, which is an invariant subgroup (cf. § 51, 1°).

‡ If G contains the group of similarity-transformations, we can assume that H_p does so too.

We now proceed to enumerate the different possible types of Sylow subgroups. In this list, the symbol P_k means "Sylow subgroup of order k."

$p=2$:

(a) P_2, generated by $(1, -1, -1)$.

(b) P_4, generated by $(1, -1, -1)$ and $(-1, 1, -1)$.

(c) P_4, generated by $(1, i, -i)$.

(d) P_8, generated by (b) and T':

$$x_1=\alpha x_1',\ x_2=\beta x_3',\ x_3=\gamma x_2'.$$

(e) P_8, generated by (c) and T'.

$p=3$:

(a) P_3, generated by $(1, \omega, \omega^2)$.

(b) $P_{3\phi}$, generated by $(\epsilon, \epsilon, \epsilon\omega^2)$, where $\epsilon^3=\omega$.

(c) $P_{9\phi}$, generated by (a) and (b).

(d) $P_{9\phi}$, generated by (a) and T'': $x_1=x_2',\ x_2=x_3',\ x_3=x_1'$.

(e) $P_{27\phi}$, generated by (b) and T''.

A group of order 5^a is abelian and contains no transformation of order 5^2 (§ 67, Corollary). If therefore $a\geqq 2$, we necessarily have two or more generating transformations, say $S_1=(a_1, a_2, a_3)$ and $S_2=(a_4, a_5, a_6)$, both of order 5. If now a represents a primitive 5th root of unity, a transformation of order 5 and variety 2 can be found in G, namely $T=S_1^aS_2^b=(a, a, a^{-2})$. (We merely determine a and b such that $a_1^aa_4^b=a_2^aa_5^b$.)

The transformation T *leaves invariant* every straight line through the point X: $x_1=x_2=0$. If R be any conjugate to T, then R would likewise leave invariant every straight line through a certain point Y. Accordingly, both T and R leave invariant the straight line which joins

X and Y. Let the variables be so changed that this line is $x_1=0$; the group generated by T and R will then be intransitive (§ 20). If the component H of this group in the variables x_2, x_3 is not primitive, T and R are commutative, because they will appear in the canonical form. Therefore, either, 1° all the transformations conjugate with T are mutually commutative, or, 2° for at least one pair of such transformations (say T and R) there is a primitive group H in two variables (x_2, x_3). This group must be of type (E), § 58, and contains the following transformation $(-\omega, -\omega^2)$. Therefore G contains the transformation $(1, -\omega, -\omega^2)$, and is not primitive (§ 70).

In the alternate case 1°, G contains invariantly the abelian group generated by T and its conjugates and is not primitive (§ 61).

Accordingly, $a=1$, and a transformation of order 5 must be of variety 3. By trial, we now find the following type:

$$P_5, \text{ generated by } (1, \alpha, \alpha^{-1}),\ \alpha^5=1.$$

A Sylow subgroup of order 7^a is abelian. By § 73, $a<2$, and by § 70, we can have no transformation of type $(\alpha^2, \alpha^2, \alpha^3)$ or $(1, \alpha, \alpha^{-1})$, where $\alpha^7=1$. Accordingly, we are limited to the following type:

$$P_7, \text{ generated by } (\beta, \beta^2, \beta^4);\ \beta^7=1.$$

The types P_5, P_7 are mutually exclusive. For, if both were present in a group, we should have a transformation of order 35 (§ 90, Exercise 2), and therefore two commutative transformations of orders 5 and 7, namely those listed above under P_5 and P_7. But this would imply a subgroup H_p (§ 68).

For the same reasons, the types (*b*), (*c*), and (*e*) for $p=3$ cannot exist simultaneously with a subgroup of order 5 or one of order 7 in a primitive group.

81. **The orders of the primitive simple groups.** Consider first the case of a group G of order $g\phi=7g_1\phi$. By §80, g_1 is a factor of $2^3.3^2\phi$, and we have 8 or 36 subgroups of order 7 (§ 36) in the corresponding collineation group. In the first case, P_7 is invariant in a group H' of order $h'=g\phi/8$ (§ 30), and in the second case it is invariant in a group of order $g\phi/36$. Now, P_7 is generated by a transformation $(\beta, \beta^2, \beta^4)$ as we have seen; it is therefore a simple matter to show that the groups of orders 63ϕ or 14ϕ would be impossible or would imply a subgroup H_p. It follows that $g=252$ or 168.

Consider next a group G of order $g\phi=5g_1\phi$, g_1 being as above a factor of $2^3.3^2$. Here we have 6 or 36 Sylow subgroups of order 5. Now, it is easily verified that such a group, generated by $(1, \alpha, \alpha^{-1})$, cannot be invariant in a subgroup H' of order $h'=20k$ or $15k$; it follows that the numbers $g/6$ and $g/36$ are either 5 or 10; i.e., g is one of the numbers 30, 60, 180, 360.

The orders to be considered are therefore 60ϕ, 360ϕ and 168ϕ (cf. § 48). There are no simple groups of order $2^a.3^b$ (§ 100).

82. **The three types of primitive simple groups.** The simple groups of orders 60 and 360 are simply isomorphic with the alternating groups on 5 and 6 letters respectively. To determine the corresponding linear groups, we construct the transformations $F_1, F_2, \ldots$, satisfying the relations specified in § 50, as was done in chap. III in the case of the group (E). We find the types:*

* Cf. Maschke, *Mathematische Annalen*, Bd. 51 (1899), pp. 264–67.

(H) Group of order 60, generated by F_1, F_2, F_3, satisfying the relations:

$$F_1^3=F_2^2=F_3^2=E,\ (F_1F_2)^3=(F_2F_3)^3=E,\ (F_1F_3)^2=E;$$

namely:

$$F_1\colon\ x_1=x_2',\ x_2=x_3',\ x_3=x_1';$$

$$F_2=(1,\ -1,\ -1);$$

$$F_3\colon\ x_1=\tfrac{1}{2}(-x_1'+\mu_2x_2'+\mu_1x_3'),\ x_2=\tfrac{1}{2}(\mu_2x_1'+\mu_1x_2'-x_3'),\ x_3=\tfrac{1}{2}(\mu_1x_1'-x_2'+\mu_2x_3');$$

where $\mu_1=\tfrac{1}{2}(-1+\sqrt{5}),\ \mu_2=\tfrac{1}{2}(-1-\sqrt{5})$.

(I) Group of order 360ϕ, generated by F_1, F_2, F_3 of (H) and F_4, where

$$F_4^2=E,\quad (F_1F_4)^2=(F_2F_4)^2=(F_3F_4)^3=E;$$

$$F_4\colon\ x_1=-x_1',\quad x_2=-\omega x_3',\quad x_3=-\omega^2x_2';\quad \omega^3=1.$$

Concerning the simple group of order 168, the generating relations can best be obtained by examining the substitution group on 7 letters simply isomorphic with the group in question.* We shall here select the substitutions $S=(abcdefg)$, $T=(adb)(cef)$, $R=(ab)(ce)$, satisfying the relations:

$$S^7=T^3=R^2=(RS)^4=E,\quad T^{-1}ST=S^4,\quad R^{-1}TR=T^2.$$

(J) Group of order 168 generated by S, T, R:

$$S=(\beta,\ \beta^2,\ \beta^4);$$

$$T\colon\ x_1=x_2',\ x_2=x_3',\ x_3=x_1';$$

$$R\colon\ x_1=h(ax_1'+bx_2'+cx_3'),\quad x_2=h(bx_1'+cx_2'+ax_3'),\quad x_3=h(cx_1'+ax_2'+bx_3');$$

where $\beta^7=1,\ a=\beta^4-\beta^3,\ b=\beta^2-\beta^5,\ c=\beta-\beta^6;$

$$h=(\beta+\beta^2+\beta^4-\beta^6-\beta^5-\beta^3)=\frac{1}{\sqrt{-7}}.$$

* Cf. Burnside, *Theory of Groups of Finite Order*, 2d ed., Cambridge, 1911, pp. 218, 310; Miller, Blichfeldt, and Dickson, *Theory and Applications of Finite Groups*, New York, 1916, p. 50.

83. **Primitive groups having invariant primitive subgroups.** A possible subgroup H_p is monomial § (80). We have already determined the primitive groups containing a group of this type invariantly; it is therefore unnecessary to consider the groups containing the subgroups H_p. Hence, the orders of the groups still to be examined must be factors of the numbers $2^3.3^3\phi$, $2^3.3^2.5\phi$, $2^3.3^2.7\phi$, as we have seen.

The group (I) has already a maximum order. Again, the group (J) cannot be invariant in a group of order $2^3.3^2.7\phi$, since a possible group of this order must contain a subgroup H_p (§ 81). As to the group (H), we make use of the fact that its 6 subgroups of order 5 must be permuted among themselves by an assumed larger group (K), in which it is self-conjugate. In any event, we would have a subgroup of order $20k$ or $30k$, containing a given P_5 self-conjugately. But this would imply a group H_p (cf. § 81).

There remain the groups (E), (F), (G). Now, any larger group would permute among themselves the four triangles which form an invariant system for these groups. But this was just the condition under which the three given groups were determined. Hence no new types result.

EXERCISES

1. Determine the linear groups in two variables by the method of this chapter. (To determine the primitive simple groups, show first that the order of such a group is a factor of 60ϕ.)

2. Obtain the group (H) by the second method given in § 58, in the following form:

$$S'=(1,\ \epsilon^4,\ \epsilon);\quad U':\ x_1=-x_1',\ x_2=-x_3',\ x_3=-x_2';$$

$$T':\quad x_1=\frac{1}{\sqrt{5}}(x_1'+x_2'+x_3'),\quad x_2=\frac{1}{\sqrt{5}}(2x_1'+sx_2'+tx_3'),$$

$$x_3=\frac{1}{\sqrt{5}}(2x_1'+tx_2'+sx_3');$$

where $\epsilon^5=1$, $s=\epsilon^2+\epsilon^3$, $t=\epsilon+\epsilon^4$, $\sqrt{5}=t-s$.

Show also that the second form of (E), § 58, transforms the variables $y_0 = -x_1x_2$, $y_1 = x_2^2$, $y_2 = -x_1^2$ into linear functions of themselves, and hence this group appears as a linear group in three variables, which is precisely the group (H) as given in this exercise if we write y_0, y_1, y_3 for x_1, x_2, x_3 respectively in (H).

3. Obtain the group (I) by adding a transformation $W = (ad)(ef)$ to the list S', U', T' of Exercise 2, and show that

$$W: \; x_1 = \frac{1}{\sqrt{5}}(x_1' + \lambda_1 x_2' + \lambda_1 x_3'), \qquad x_2 = \frac{1}{\sqrt{5}}(2\lambda_2 x_1' + s x_2' + t x_3'),$$

$$x_3 = \frac{1}{\sqrt{5}}(2\lambda_2 x_1' + t x_2' + s x_3');$$

where $\lambda_1 = \frac{1}{4}(-1 \pm \sqrt{-15})$, $\qquad \lambda_2 = \frac{1}{4}(-1 \mp \sqrt{-15})$.

4. Show that the function $x_1^3x_3 + x_2^3x_1 + x_3^3x_2$ is invariant under (J).

5. In § 80 it was shown that two transformations, both of variety 2, would generate an intransitive group. By the same process (geometrical), prove that two transformations in four variables, both of variety 2, would also generate an intransitive group.

Bibliography.—Complete discussions of the linear groups in three variables are to be found in the following articles: Jordan, *Journal für die reine und angewandte Mathematik*, Bd. 84 (1878), pp. 125 ff.; Valentiner, *De endelige Transformations-Gruppers Theori*, Copenhagen (Videnskabernes Selskabs Afhandlinger), 1889; Mitchell, *Transactions of the American Mathematical Society*, XII (1911), 207–42; and the author, *Transactions of the American Mathematical Society*, V (1904), 321–25, and *Mathematische Annalen*, Bd. 63 (1907), pp. 552–72. See also Miller, Blichfeldt, and Dickson, *Theory and Applications of Finite Groups*, § 125, where further references will be found.

CHAPTER VI

THE THEORY OF GROUP CHARACTERISTICS

84. **Introduction.** This theory, of importance not only for linear groups, but for abstract and substitution groups as well, was initiated by Frobenius and is largely due to him,* though Schur† and Burnside‡ simplified the theory and added extensive applications. We shall devote this chapter to an exposition of the main points of the theory by a process differing in many respects from previous expositions.

It is not assumed in this chapter that the transformations of a linear group under discussion are necessarily of determinant unity.

For the sake of uniformity of notation, we shall throughout this chapter denote the order of a group under discussion by g (unless otherwise specified), however the group may be designated (G, G', H, etc.) Furthermore, the number of its sets of conjugate operators (§ 29) shall be denoted by h, these sets to contain respectively $g_1, g_2, \ldots, g_h$ operators, so that $g = g_1 + g_2 + \ldots + g_h$.

* *Sitzungsberichte der Kgl.-Preussischen Akademie der Wissenschaften*, 1896, pp. 985, 1343; 1897, p. 994; 1899, p. 482.

† *Sitzungsberichte*, etc., 1905, p. 406; *Journal für die reine und angewandte Mathematik*, Bd. 127 (1904), pp. 20–50; Bd. 132 (1907), pp. 85–137; Bd. 139 (1911), pp. 155–250.

‡ *Acta Mathematica*, XXVIII (1904), 369–87; *Proceedings of the London Mathematical Society*, 1904, pp. 117–23; *Theory of Groups of Finite Order*, 2d ed., Cambridge, 1911, pp. 243 ff.

See also the following accounts: Molien, *Sitzungsberichte*, etc., 1897, pp. 1152–56; Dickson, *Annals of Mathematics*, 1902, pp. 25–49; Miller, Blichfeldt, and Dickson, *Theory and Applications of Finite Groups*, New York, 1916, pp. 257–78; and the author, *Transactions of the American Mathematical Society*, V (1904), 461–66.

85. **Remarks on intransitive groups.—Extension of group-concept.** 1°. Let $G=(S_1, S_2, \ldots, S_g)$ be an intransitive group, which upon a suitable change of variables breaks up into two or more groups, $G', G'', \ldots$, corresponding to the various sets of intransitivity. We shall have occasion to employ a notation analogous to that used for linear transformations, namely,

$$G=\begin{bmatrix} G' & 0 & 0 & . \\ 0 & G'' & 0 & . \\ 0 & 0 & G''' & . \\ . & . & . & . \end{bmatrix};$$

and we shall say that $G', G'', \ldots$ are "component" groups of G.

2°. Under certain conditions it is convenient to extend the name "group" to a set of operators which are not all distinct, but which can be put into a (1, 1) correspondence with a group G. A group G' of order g' which is $(1, h)$ isomorphic with G can be exhibited as if it were a group simply isomorphic with G, namely by repeating each of its operators h times. For instance, the substitution group of order 6: E, (ab), (ac), (bc), (abc), (acb) is multiply isomorphic with two of its subgroups: E; and E, (ab). With the concept of "group" extended as indicated above, we may exhibit the three groups as simply isomorphic in the following manner:

$$\begin{array}{llllll} E, & (ab), & (ac), & (bc), & (abc), & (acb); \\ E, & E, & E, & E, & E, & E; \\ E, & (ab), & (ab), & (ab), & E, & E. \end{array}$$

We shall accordingly agree to look upon the groups G, $G', G'', \ldots$ in 1° as simply isomorphic.

86. **Characteristics.** 1°. *Definition.*—Let the variables of the group $G=(S_1, S_2, \ldots, S_g)$ be $x_1, x_2, \ldots, x_n$.

As noted in § 23, the sum of the multipliers of a given transformation S_t is called the *characteristic* of S_t, and we shall here denote it by χ_t or $\chi(S_t)$. It is equal to the sum of the elements in the principal diagonal of S_t; if S_t is written in canonical form: $(\alpha, \beta, \ldots, \lambda)$, then $\chi_t = \alpha + \beta + \ldots + \lambda$. Thus, $\chi(E) = n$.

2°. *Inverse and conjugate-imaginary transformations.*—The multipliers are always roots of unity, and if $\alpha, \beta, \ldots$ are the multipliers of S_t, those of S_t^{-1} are the reciprocals $\alpha^{-1}, \beta^{-1}, \ldots$. Since the reciprocal of a root of unity α is its conjugate-imaginary ($\alpha^{-1} = \bar{\alpha}$), we have

$$\bar{\chi}_t = \chi(\bar{S}_t) = \bar{\alpha} + \bar{\beta} + \ldots = \alpha^{-1} + \beta^{-1} + \ldots = \chi(S_t^{-1}).$$

3°. *Conjugate transformations.*—The characteristics of conjugate transformations are equal (§ 23). Hence, if there are h complete conjugate sets of transformations in G (§ 29), there cannot be more than h different characteristics of G. In conformity with the notation adopted in § 84, we shall indicate these by the symbols $\chi_1, \chi_2, \ldots, \chi_h$.

4°. *Intransitive groups.*—The characteristic of a transformation S of the intransitive group G, § 85, 1°, is evidently the sum of the characteristics of the "component" transformations $S', S'', \ldots$:

$$\chi(S) = \chi(S') + \chi(S'') + \ldots$$

5°. *Substitution groups.*—When a substitution consisting of a single cycle on more than one letter, $S = (a_1 a_2 \ldots a_m)$, is written in matrix form as a linear transformation (§ 1), the elements in its principal diagonal are all zero. Hence its characteristic is zero. If $m = 1$, the transformation has the form $S = (1)$; in this case $\chi(S) = 1$. The multipliers of $S = (a_1 a_2 \ldots a_m)$ are the m different mth roots of unity; thus, the substitution $S = (a_1 a_2 a_3)$, when written as a linear transformation in canonical form, becomes $S = (1, \omega, \omega^2)$, where $\omega^3 = 1$.

It follows that the characteristic of the most general substitution S on n letters is the integer which equals the number of cycles of one letter; i.e., $\chi(S)$ = the number of letters that the substitution leaves unchanged. In particular, the characteristics of a regular group (§ 47) are all zero, except that $\chi(E)$ equals the order of the group.

Frobenius and Schur call the set of quantities $\chi_1, \ldots, \chi_g$ a *character* of G. In their terminology, an abstract group G would possess as many *simple* characters as there are non-equivalent linear groups to which G is simply or multiply isomorphic (cf. § 99).

87. **The sum and product of matrices.** The *sum* of a series of square matrices of the same order is the matrix whose elements are the algebraic sums of the corresponding elements of the given matrices. Thus,

$$\begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ c_1+c_2 & d_1+d_2 \end{bmatrix}.$$

If $S_1, S_2, \ldots$ are linear transformations in the same variables, we shall write $S_1+S_2+\ldots$ to denote the matrix which is the sum of the matrices of $S_1, S_2, \ldots$

The *product* of two matrices is obtained by the rule given in § 3, irrespective of whether the matrices represent linear transformations or not. If M represents a matrix, and c a constant or a variable, the symbol cM shall represent the matrix obtained by multiplying every element of M by c.

In accordance with these definitions we find

$$S_1+S_2 = S_2+S_1,$$

$$T(S_1+S_2+\ldots) = TS_1+TS_2+\ldots,$$

$$T^{-1}(S_1+S_2+\ldots)T = T^{-1}S_1T+T^{-1}S_2T+\ldots,$$

$$(S_1+S_2+\ldots)(T_1+T_2+\ldots) = S_1T_1+S_1T_2+S_2T_1 + S_2T_2+\ldots,$$

$$c(S_1+S_2+\ldots) = cS_1+cS_2+\ldots.$$

Again, if X represents a linear function of the variables $x_1, x_2, \ldots, x_n$, and if the matrix M be regarded as the matrix of a linear transformation (though the determinant of M may vanish), we shall by $(X)M$ represent the result of operating upon X by M (cf. § 2). Now if

$$M = S_1 + S_2 + \ldots + S_m,$$

where $S_1, \ldots, S_m$ are linear transformations of a group in the variables $x_1, \ldots, x_n$, it is then readily seen that

$$(X)M = (X)S_1 + (X)S_2 + \ldots + (X)S_m.$$

88. **Invariants.** A function $f(x_1, \ldots, x_n)$ which is transformed into a constant multiple of itself by every transformation of a group G is called an *invariant* of G. It is an *absolute* invariant if the constant multiplier is unity for every transformation of G; otherwise it is a *relative* invariant.

A series of invariants $f_1, \ldots, f_m$ are said to be *independent* of each other if the variables cannot be eliminated from the equations

$$f_1 = a_1, \ \ldots, \ f_m = a_m,$$

where $a_1, \ldots, a_m$ are arbitrary constants. They are said to be *linearly independent* if no identity exists of the form

$$b_1 f_1 + \ldots + b_m f_m = 0,$$

where $b_1, \ldots, b_m$ are constants, not all zero.

EXERCISES

1. The substitution group E, $(x_1x_2)(x_3x_4)$, $(x_1x_3)(x_2x_4)$, $(x_1x_4)(x_2x_3)$ is abelian and consequently intransitive when written as a linear group (§ 22). Write it in canonical form, and show that it possesses four invariants of the first degree, one of which is absolute. Show also that the characteristics are 4, 0, 0, 0.

2. Write the symmetric group on three letters as a linear group, and construct the matrices which are each the sum of the

transformations of a conjugate set. Then show that any one of these matrices (M) and any transformation (S) of the group are commutative: $MS=SM$. Show also that the matrices are mutually commutative.

3. Write down the characteristics of the group in the previous exercise, and prove that their sum, the sum of their squares, the sum of their cubes, etc., is always a multiple of 6, the order of the group.

4. Construct the two independent invariants of the first degree of the group of order 6 in § 95.

Prove also that the alternating group on 5 letters possesses only one invariant of the first degree.

5. Prove that the characteristics of the two transformations AB and BA are equal.

ON THE CHARACTERISTICS OF TRANSITIVE GROUPS, §§ 89–91

89. **Theorem 1.** *If* $S_1, \ldots, S_m$ *are the different transformations of a conjugate set of a transitive linear group* G *in* n *variables, then the matrix*

$$M=S_1+\ \ldots\ +S_m$$

is commutative with every transformation of G *and has the form of a similarity-transformation* $(\alpha, \alpha, \ldots, \alpha)$, *where* $\alpha=m\chi(S_1)/n$.

Proof.—That M is commutative with any given transformation T of G is seen as follows. We have

$$T^{-1}MT=T^{-1}S_1T+T^{-1}S_2T+\ \ldots\ =S_1+S_2+\ \ldots\ =M,$$

since $T^{-1}S_1T, \ldots, T^{-1}S_mT$ are the transformations $S_1, \ldots, S_m$ over again in some order (§ 29, (c)). Hence $MT=TM$.

We shall proceed to prove the second part of the theorem. By the method of § 21, we can find a linear function of the variables of the group which is an invariant of M, say $(x_1)=\alpha x_1$, where α is a constant (possibly zero).

There may be other linear functions $x_2, \ldots$ such that

$$(x_2)M = \alpha x_2, \ \ldots ;$$

let $x_1, x_2, \ldots, x_k$ be all those that have this property and are linearly independent. We shall indicate this fact symbolically by $(x_1, \ldots, x_k)M = \alpha(x_1, \ldots, x_k)$. It is plain that a linear function having this property must be a linear function of the variables $x_1, \ldots, x_k$.

Now let T be any transformation of G, and let

$$(x_1)T = y_1, \quad (x_2)T = y_2, \quad \ldots, \quad (x_k)T = y_k.$$

Then, since $(x_1, \ldots, x_k)MT = (x_1, \ldots, x_k)TM$, we have

$$\alpha(y_1, \ldots, y_k) = (y_1, \ldots, y_k)M,$$

so that $y_1, \ldots$ have the property ascribed above to $x_1, \ldots$. It follows that $y_1, \ldots$ are linear functions of $x_1, \ldots$; that is, the latter variables form an intransitive set of G (§ 20), unless $k = n$. Hence, since G is transitive, $k = n$, and M has the form of a similarity-transformation $(\alpha, \alpha, \ldots, \alpha)$.

Finally, to find the value of α, we observe from the formation of M that the sum of the elements of its principal diagonal, $n\alpha$, equals the sum of the characteristics of $S_1, \ldots, S_m$. But these are all equal (§ 86, 3°); hence $n\alpha = m\chi(S_1)$.

90. **Theorem 2.** *Let the number of transformations in the h different conjugate sets of a transitive group G in n variables be $g_1, g_2, \ldots, g_h$, and let the corresponding characteristics be denoted by $\chi_1, \chi_2, \ldots, \chi_h$ (§ 86, 3°). Then*

$$(1) \quad \left(\frac{g_s\chi_s}{n}\right)\left(\frac{g_t\chi_t}{n}\right) = \sum_{v=1}^{h} c_{stv}\left(\frac{g_v\chi_v}{n}\right) \qquad (s, t = 1, 2, \ldots, h),$$

where $c_{stv}, \ldots$ represent certain positive integers or zero.

Proof.—Let the sum of the matrices of the g_k transformations of the kth set be denoted by M_k. Then

$$M_s M_t = c_{st1} M_1 + c_{st2} M_2 + \ . \ . \ + c_{sth} M_h \quad (s, \ t = 1, \ 2, \ . \ . \ , h). \tag{2}$$

For the $g_s g_t$ matrices in the product $M_s M_t$ must make up one or more conjugate sets, since $T^{-1}(M_s M_t)T = (T^{-1}M_s T)(T^{-1}M_t T) = M_s M_t$. Accordingly, this product is the sum of one or more of the matrices $M_1, \ . \ . \ , M_h$, possibly repeated a certain number of times.

We now substitute in (2) the canonical forms of the matrices $M_1, \ . \ . \ , M_h$ as given by Theorem 1, and obtain the equation $(\beta, \ . \ . \ , \beta) = (\gamma, \ . \ . \ \gamma, \ )$, where β has for value the left-hand member of (1), and γ the right-hand member.

COROLLARY. *If a transitive linear group G in n variables contains two characteristics χ_s, χ_t such that the sum of the n^2 roots in the product $\chi_s \chi_t$ cannot be written as a sum in which primitive roots of index k are absent, then there is in G a characteristic containing roots of index k and therefore a transformation whose order is k or a multiple of k.**

This follows from the equation (1). By the conditions of the corollary, at least one of the characteristics χ_v of the right-hand member must contain roots of index k. There is, therefore, a transformation whose order is divisible by k. For, the order m of a transformation $S = (\alpha, \beta, \ . \ . \ )$ is the least common multiple of the indices of the roots $\alpha, \ \beta, \ . \ . \ .$, since $S^m = (1, \ 1, \ . \ . \ ) = (\alpha^m, \beta^m, \ . \ . \ )$.

To illustrate, let $\chi_s = -1 + i + i$ and $\chi_t = \alpha + \alpha + \alpha^3$, where $i = \sqrt{-1}$ and α is a primitive fifth root of unity. Here $\chi_s \chi_t$, or $4i\alpha + 2i\alpha^3 - 2\alpha - \alpha^3$, cannot be written as a

*Burnside, *Theory of Groups*, 2d ed., p. 347.

sum which is free from roots of index 20 (namely $i\alpha$, $i\alpha^2$, etc.) by Kronecker's theorem (§ 133, 6°).

EXERCISES

1. Selecting the h equations (1) obtained by keeping s fixed while taking $t=1, 2, \ldots, h$, prove that $g_s\chi_s/n$ is an algebraic integer (Frobenius).

2. Prove that if a group in n variables contains transformations of orders p and q, two different prime numbers both greater than $n+1$, then the group contains a transformation of order pq.

91. **Theorem 3.** *The sum of the characteristics of a transitive group in n variables, $n \geqq 2$, is zero.*

Proof.—Let, as in § 90, the group G contain h conjugate sets, and let M_k represent the sum of matrices in the kth set. By § 89, the matrices $M_1, \ldots, M_h$ all have the form of a similarity-transformation; the same will therefore be the case with the sum M of all the matrices in G, which is $M_1+M_2+\ldots+M_h$, say $M=(\epsilon, \epsilon, \ldots, \epsilon)$. Now, if S is any transformation of G distinct from the identity, the relation $MS=M$ (§ 27, Exercise 3) is found to imply $\epsilon=0$. Hence,

$$g_1\chi_1+g_2\chi_2+\ldots+g_h\chi_h=0.$$

When $n=1$, two cases arise. If the group consists of E repeated g times (§ 85, 2°), the sum in question is g; if the transformations are not all the identity, the sum vanishes. For an illustration take the group of order $4m$ (each of the following transformations repeated m times): $E=(1)$, $S=(i)$, $S^2=(-1)$, $S^3=(-i)$; $i=\sqrt{-1}$.

Combining these results and referring to § 86, 4°, and § 85, 1°, we get the

COROLLARY. *The sum of the characteristics of an intransitive group G is its order multiplied by the integer representing the total number of the component groups*

in G whose transformations are the identity repeated g times.

It is plain that to each group in G of the latter type we have an absolute invariant of the first degree, and vice versa. Hence we may state the preceding corollary in the following form: *the sum of the characteristics of a group G is its order multiplied by the total number of independent absolute invariants of G of the first degree.*

EXERCISE

Prove that the average number of letters which remain unchanged by a substitution of a transitive substitution group G is equal to unity. (Hint: Prove that G possesses a single absolute invariant of the first degree.)

ON THE CHARACTERISTICS OF ISOMORPHIC GROUPS, §§ 92–94

92. **Composition of two groups.** Let G' and G'' be two simply isomorphic groups in respectively n and m variables, say $x_1, \ldots, x_n$, and $y_1, \ldots, y_m$. Then the nm products $x_1y_1, \ldots, x_ny_m$ are transformed into linear functions of themselves when operated upon simultaneously by two corresponding transformations S' and S''. Hence, regarding these combined transformations as a single linear transformation S in the nm variables, we obtain a linear group G simply isomorphic with G' and G''. For, to E of G' and G'' will correspond E of G, and if $S'_pS'_q=S'_r$, $S''_pS''_q=S''_r$, we have $S_pS_q=S_r$. We shall say that G is *compounded* from the groups G' and G''.

LEMMA 1. *The characteristic of a transformation S contained in a group G which is compounded from the groups G' and G'', is equal to the product of the characteristics of the corresponding transformations S' and S''.*

This is seen immediately when S' and S'' are both written in the canonical form, which can obviously be

done. If then $(x_a)S' = \alpha_a x_a$, $(y_b)S'' = \beta_b y_b$, we find $(x_a y_b)S = \alpha_a \beta_b (x_a y_b)$, so that

$$\chi(S) = \sum_{a=1}^{n} \sum_{b=1}^{m} \alpha_a \beta_b = \left(\sum_{a=1}^{n} \alpha_a \right) \left(\sum_{b=1}^{m} \beta_b \right) = \chi(S') \cdot \chi(S'') .$$

LEMMA 2. *Let there be given an invariant of G:*

$$f = X_1 Y_1 + \ . \ . \ . \ + X_k Y_k,$$

where $X_1, \ . \ . \ , X_k$ are linear functions of $x_1, \ . \ . \ , x_n$ and $Y_1, \ . \ . \ , Y_k$ linear functions of $y_1, \ . \ . \ , y_m$. Then if $k < n$, the group G' is intransitive.

Proof.—For the sake of simplicity take $k = 3$, say $f = X_1 Y_1 + X_2 Y_2 + X_3 Y_3$. We may assume that X_1, X_2, X_3 (as well as Y_1, Y_2, Y_3) are linearly independent of each other; if it were possible to write, say, $X_3 = a_1 X_1 + a_2 X_2$, the function f could be expressed in two terms:

$$X_1(Y_1 + a_1 Y_3) + X_2(Y_2 + a_2 Y_2) = X_1 Y_1'' + X_2 Y_2''.$$

A transformation of G' will change X_1, X_2, X_3 into there linearly independent functions of $x_1, \ . \ . \ , x_n$, and the corresponding transformations of G'' will change Y_1, Y_2, Y_3 into three linearly independent functions of $y_1, \ . \ . \ , y_m$. Let the resulting expression be

$$f' = X_1' Y_1' + X_2' Y_2' + X_3' Y_3',$$

and we should have $f \equiv f'$. But this implies that X_1', X_2', X_3' are linear functions of X_1, X_2, X_3. Hence, if $n > 3$, G' is reducible and accordingly intransitive.

93. **Theorem 4.** *Let a transitive group G be compounded with its conjugate-imaginary group $\bar{G}$. The resulting group is intransitive, and among the component groups into which it breaks up will be found just one group*

made up of the identity repeated g times. Hence (Corollary, § 91),

$$(3) \qquad g_1\chi_1\bar{\chi}_1+g_2\chi_2\bar{\chi}_2+\ .\ .\ +g_h\chi_h\bar{\chi}_h=g.$$

Proof.—Let the compounded group be denoted by H. Its characteristics are $\chi_t\bar{\chi}_t$ (Lemma 1, § 92); and their sum Σ (i.e., the left-hand member of (3)), divided by g, represents the number of absolute invariants of H of the form $X_1\bar{X}_1+\ .\ .\ +X_n\bar{X}_n$ (Corollary, § 91); or, as we may write it by a proper distribution of the terms,

$$f=X_1\bar{x}_1+.\ .\ +X_n\bar{x}_n.$$

We know one such invariant already, namely the Hermitian invariant (§ 18), and we may assume that the variables are originally so chosen that this invariant is

$$I=x_1\bar{x}_1+x_2\bar{x}_2+\ .\ .\ +x_n\bar{x}_n.$$

Then if λ is any constant, the expression

$$f+\lambda I=(X_1+\lambda x_1)\bar{x}_1+(X_2+\lambda x_2)\bar{x}_2+\ .\ .\ +(X_n+\lambda x_n)\bar{x}_n$$

is also an invariant.

Now, the constant λ may always be determined such that $X_1+\lambda x_1, \ .\ .\ , X_n+\lambda x_n$ are not linearly independent. (For an illustration, take $n=2, X_1=px_1+qx_2, X_2=rx_1+sx_2$. Here λ is a solution of the equation $\begin{vmatrix} p+\lambda & q \\ r & s+\lambda \end{vmatrix}=0$.) Therefore either G' is intransitive (Lemma 2, § 92), or $f+\lambda I$ vanishes identically. Hence, since the first alternative violates the assumption of the theorem, any invariant f of H is merely a constant multiple of I (viz., $f=-\lambda I$); in other words, the number Σ/g of linearly independent invariants of H is unity. The theorem follows by § 91.

COROLLARY. *The number of variables n of a transitive linear group G is a factor of the order g.*

Proof.—Dividing the equation (3) by n we get

$$\frac{g}{n}=\frac{g_1\chi_1}{n}\bar{\chi}_1+\frac{g_2\chi_2}{n}\bar{\chi}_2+\ .\ .\ +\frac{g_h\chi_h}{n}\bar{\chi}_h.$$

The quantities $\frac{g_t\chi_t}{n}$ are algebraic integers (Exercise 1, § 90), as well as the quantities $\bar{\chi}_t$. Hence, since the sums and products of algebraic integers are again algebraic integers, it follows that g/n is an algebraic integer; i.e., g/n is an ordinary integer (§ 134).

94. **Theorem 5.** *Let G' and G'' be two simply isomorphic transitive groups, whose corresponding characteristics are χ'_t and χ''_t. Then the sum*

$$(4)\qquad g_1\chi'_1\bar{\chi}''_1+g_2\chi'_2\bar{\chi}''_2+\ .\ .\ +g_h\chi'_h\bar{\chi}''_h$$

equals g or zero, according as the two groups are equivalent or not.

Proof.—If they are equivalent, the variables of G'' may be chosen so that the groups are identical, and the conjugate-imaginary groups $\bar{G}'$ and $\bar{G}''$ will be identical also. The sum (4) is then equal to g, by Theorem 4.

Conversely, if the sum equals g, the two groups are equivalent, as we shall proceed to prove. Let the variables of G' and G'' be respectively $x_1, \ .\ .\ , x_n; y_1, \ .\ .\ , y_m$; and suppose that $n\leqq m$. The expression (4), divided by g, equals the number of absolute invariants of the form $X_1\bar{Y}_1+X_2\bar{Y}_2+\ .\ .\ .$ of the group G compounded from G' and $\bar{G}''$ (§ 91). Since there is one such, $n=m$ (Lemma 2, § 92), and we may choose the variables of G'' so that the invariant has the form

$$I=x_1\bar{y}_1+x_2\bar{y}_2+\ .\ .\ +x_n\bar{y}_n.$$

But this is the form of the invariant of the group H compounded from G' and its conjugate-imaginary group $\bar{G}'$, after the variables of the latter group have been

written $\bar{y}_1, \ldots, \bar{y}_n$ in place of $\bar{x}_1, \ldots, \bar{x}_n$. It is therefore an easy matter to prove that the groups $\bar{G}''$ and $\bar{G}'$ are identical. For, let S', $\bar{S}'$, $\bar{S}''$ be corresponding transformations of G', $\bar{G}'$, $\bar{G}''$, and we have $(I)\bar{S}'S' \equiv (I)\bar{S}''S'$, so that $(I)\bar{S}' \equiv (I)\bar{S}.''$ (The transformations S' and $\bar{S}'$, as well as S' and $\bar{S}''$, are commutative, since the variables of the respective groups are independent of each other.) It follows directly that $\bar{S}'$ and $\bar{S}''$ are identical.

Finally, we cannot have more than one invariant of the form I above, since otherwise the groups G' and G'' would be intransitive (cf. proof of Theorem 4). Accordingly, the sum (4) is either g or zero.

COROLLARY 1. *If the corresponding characteristics of two simply isomorphic groups are equal, the groups are equivalent.*

COROLLARY 2. *Let χ_t' and χ_t'' be corresponding characteristics of two groups, G' and G'', the first of which is transitive. The sum* (4), *divided by g, will in this case represent the number of components in the group G'' which are equivalent to G', when the former is broken up into its ultimate sets of intransitivity.*

We write G'' in such an ultimate intransitive form (cf. § 85, 1°), and apply § 86, 4°, and Theorem 5.

EXERCISES

1. Let H' and H'' be two simply isomorphic intransitive groups, and let their corresponding characteristics be denoted by χ_t' and χ_t''. Then when these groups are split up into component transitive groups, the latter may not all be non-equivalent. Let us suppose that $G_1, G_2, \ldots, G_n$ represent types of all the non-equivalent groups obtained, there being a_1 and b_1 of the first type in H' and H'' respectively, a_2 and b_2 of the second type, etc.

Now prove that the sum (4), § 94, is here equal to the integer $g(a_1b_1+a_2b_2+ \ldots +a_nb_n)$.

2. Prove that if a transitive linear group of order g in n variables contains a subgroup of order f composed of similarity-transformations, then g is divisible by fn (Schur). (Hint: Prove

first that if χ_t does not vanish, there will be f distinct sets of conjugate transformations for which the products $g_t\chi_t\bar{\chi}_t$ in (3), § 93, have the same value.)

3. Prove that a group G containing a subgroup P of order p, a prime number $\geqq n^2/(n-1)$, is intransitive, unless P is invariant in a larger subgroup of G. (Hint: With reference to the sum (3), prove that the sum of the terms $\chi_t\bar{\chi}_t$ corresponding to the transformations of order p in P alone is $\geqq np-n^2$, by Exercise 1 above. Hence prove that the sum of such terms from all the subgroups conjugate to P and from the identity exceeds g.)

ON THE TOTALITY OF NON-EQUIVALENT ISOMORPHIC GROUPS, §§ 95–99

95. **The regular group.** We shall now consider the regular substitution group H (§ 47). Regarded as a linear group, it is intransitive, since it possesses an absolute invariant of the first degree, namely the sum of the letters of substitution.

As an illustration, take the regular group on the letters $x_1, \ldots, x_6$, simply isomorphic with the symmetric group on three letters. Its substitutions are as follows:

$$S_1 = E, \qquad S_4 = (x_1x_4)(x_2x_6)(x_3x_5),$$
$$S_2 = (x_1x_2x_3)(x_4x_5x_6), \qquad S_5 = (x_1x_5)(x_2x_4)(x_3x_6),$$
$$S_3 = (x_1x_3x_2)(x_4x_6x_5), \qquad S_6 = (x_1x_6)(x_2x_5)(x_3x_4).$$

If we now introduce new variables $z_1, \ldots, z_6$, where

$$z_1 = x_1+x_2+x_3+x_4+x_5+x_6, \qquad z_4 = x_4+\omega^2x_5+\omega x_6,$$
$$z_2 = x_1+x_2+x_3-x_4-x_5-x_6, \qquad z_5 = x_4+\omega x_5+\omega^2x_6,$$
$$z_3 = x_1+\omega x_2+\omega^2x_3, \qquad z_6 = x_1+\omega^2x_2+\omega x_3,$$

the transformations of H will all be of the following type:

$$(5) \qquad \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 \\ 0 & b & 0 & 0 & 0 & 0 \\ 0 & 0 & c & d & 0 & 0 \\ 0 & 0 & e & f & 0 & 0 \\ 0 & 0 & 0 & 0 & c & d \\ 0 & 0 & 0 & 0 & e & f \end{bmatrix},$$

showing that H is split up into 4 component transitive groups in respectively 1, 1, 2, 2 variables. The groups in the variables z_3, z_4 and z_5, z_6 are equivalent, both being generated by the transformations $S_2=(\omega^2, \omega)$, $S_4=\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$. Hence, there are three non-equivalent groups.

In general, a regular group H on g letters, when written as a linear group in g variables, is intransitive. Corresponding to its ultimate sets of intransitivity we have a number of component transitive linear groups, which are not all non-equivalent. If we select a representative of each set of equivalent groups, we get, say, k representatives, forming a *set* of *non-equivalent component groups* of H. Let them be denoted by $H', H'', \ldots, H^{(k)}$, and their corresponding characteristics by $\chi_t', \chi_t'', \ldots, \chi_t^{(k)}$. Hence, if H contains n' groups equivalent to H', n'' group equivalent to H'', . . . , the characteristic of the transformation S_t of H is (§ 86, 4°)

$$\chi(S_t)=n'\chi_t'+n''\chi_t''+\ \ldots\ +n^{(k)}\chi_t^{(k)}, \tag{6}$$

and this sum is $=g$ or $=0$, according as $S_t=E$ or $S_t\neq E$ (§ 86, 5°).

96. **Theorem 6.** *Let G be a transitive linear group in n variables, and let H be a regular substitution group on g letters simply isomorphic with G. Then among the component transitive groups into which H breaks up, there are just n groups equivalent to G.*

The theorem follows from Corollary 2, § 94, if we let G and H represent G' and G'' respectively. The sum (4) will here be equal to ng (cf. § 95).

The number k of non-equivalent component groups of H is equal to h (§ 99). Anticipating this result, we can now say that *the number of non-equivalent transitive linear groups to which a given transitive linear group G*

is simply or multiply isomorphic (cf. §§ 32, 85) is equal to the number of sets of conjugate transformations of G.

EXERCISE

Let the component groups $H', \ldots, H^{(k)}$ of H contain respectively $n', n'', \ldots, n^{(k)}$ variables. Prove that (cf. Exercise 1, § 94)

$$g=(n')^2+(n'')^2+\ \ldots\ +(n^{(k)})^2.$$

At least one of the numbers $n', \ldots$ is unity. If there is more than one, then H possesses a relative invariant and is not simple.

97. **Theorem 7.** *Given any two transformations S_s and S_t of H. The sum*

$$\chi'_s\chi'_t+\chi''_s\chi''_t+\ \ldots\ +\chi^{(k)}_s\chi^{(k)}_t\equiv\Sigma$$

vanishes if S_s is not conjugate to S_t^{-1}; if these two transformations both belong to the conjugate set denoted by the subscript s, then $\Sigma=g/g_s$.

Proof.—Let the equation (1), § 90, be multiplied by n^2, and a corresponding equation formed for every one of the non-equivalent groups $H', \ldots, H^{(k)}$ of H. The constants c_{stv} are the same for each of these groups, since they are the same for all simply isomorphic groups. Hence, adding the resulting k equations, the left-hand member of the new equation, say $F_1=F_2$, will be $g_sg_t\Sigma$, and the right-hand member the expression

$$\sum_{w=1}^{k}\left\{\sum_{v=1}^{h}c_{stv}(g_vn^{(w)}\chi^{(w)}_v)\right\}=\sum_{v=1}^{h}c_{stv}\ g_v\left\{\sum_{w=1}^{k}n^{(w)}\chi^{(w)}_v\right\}\ .$$

Now, $\sum_{w=1}^{k}n^{(w)}\chi^{(w)}_v$ is the sum (6), § 95, for the subscript v. Hence, this sum vanishes or is equal to g, according as S_v does not or does represent the identity. Moreover,

in the latter case $g_v = 1$. Accordingly, the right-hand member is equal to gc_{st1}, under the assumption that $S_1 = E$.

The value of c_{st1} is found from (2), § 90, and represents the number of times the transformation E occurs in the product $M_s M_t$. Now, let R be a transformation of M_s. If R^{-1} is found in M_t, then it is readily seen that M_t is the sum of the inverses of the transformations of M_s; in that case E will occur g_s times in the product $M_s M_t$, and $g_s = g_t = c_{st1}$. On the other hand, if R^{-1} does not occur in M_t, neither will the inverse of any transformation in M_s; in this case $c_{st1} = 0$. Interpreting the equation $F_1 = F_2$ under these results we finally prove the theorem.

The second alternative in Theorem 7 can evidently be stated in the form (cf. § 86, 2°):

$$\chi_s' \bar{\chi}_s' + \chi_s'' \bar{\chi}_s'' + \ . \ . \ + \chi_s^{(k)} \bar{\chi}_s^{(k)} = g/g_s.$$

EXERCISES

1. Prove that the set of non-equivalent groups simply isomorphic with the alternating group on 5 letters consists of the group (H), § 82; the group (H_1) obtained by interchanging the numbers μ_1 and μ_2 in (H); and two groups in 4 and 5 variables respectively.

2. Prove that the group (H), § 82, compounded with its conjugate-imaginary, splits up into three transitive groups, one in 1 variable (the identity repeated 60 times, corresponding to the Hermitian invariant), one in 3 variables, and one in 5 variables.

98. **Group-matrix.** Let $x_1, \ . \ . \ , x_n$ be the variables of a transitive or intransitive group $G = (S_1, \ . \ . \ , S_g)$, and let $y_1, \ . \ . \ , y_g$ be g variables, independent of each other and of $x_1, \ . \ . \ , x_n$. Then the matrix (cf. § 87)

$$M = y_1 S_1 + y_2 S_2 + \ . \ . \ + y_g S_g$$

is called the *group-matrix* of the group G. Thus, the

group-matrix of the regular group H of order 6 given in § 95 has the form

$$M=\begin{bmatrix} y_1 & y_2 & y_3 & y_4 & y_5 & y_6 \\ y_3 & y_1 & y_2 & y_5 & y_6 & y_4 \\ y_2 & y_3 & y_1 & y_6 & y_4 & y_5 \\ y_4 & y_5 & y_6 & y_1 & y_2 & y_3 \\ y_5 & y_6 & y_4 & y_3 & y_1 & y_2 \\ y_6 & y_4 & y_5 & y_2 & y_3 & y_1 \end{bmatrix}. \tag{7}$$

The n^2 elements in M are linear homogeneous functions of $y_1, \ldots, y_g$. These functions may not all be independent of each other; thus, there are only 6 independent elements in M of (7). Bearing in mind the definitions of § 85, 2°, we shall prove the following:

THEOREM 8. *Let H', H'', . . . , $H^{(k)}$ form a complete set of non-equivalent, simply isomorphic, transitive linear groups in respectively n', n'', . . . , $n^{(k)}$ variables. Then the $(n')^2+(n'')^2+\ldots+(n^{(k)})^2=g$ elements contained in the k group-matrices $y_1S_1+\ldots+y_gS_g$ of these groups are all independent functions of the variables $y_1, \ldots, y_g$.*

Proof.—Consider the group-matrix M of the regular group H of which H', H'', . . . , $H^{(k)}$ are component non-equivalent groups. The matrix M will, while H has still the form of a substitution group, contain just g independent elements. For, each element will consist of a single letter y_j, as may be proved easily (cf. § 47).

Now let H be broken up into its different component groups by means of a linear transformation T (cf. § 13). Correspondingly M is transformed by T into a new matrix M':

$$T^{-1}MT=T^{-1}(y_1S_1+\ldots+y_gS_g)T=$$
$$y_1(T^{-1}S_1T)+\ldots+y_g(T^{-1}S_gT)=M'.$$

The elements of M' are linear functions of the elements of M, and vice versa; the coefficients being functions of the elements of T. Hence there are as many independent functions of $y_1, \ldots, y_g$ among the elements of M' as among the elements of M; namely g.

Now, each non-equivalent component group $H^{(j)}$ is repeated as an equivalent group $n^{(j)}$ times (§ 96), and these equivalent groups can be made identical by a proper modification of T. Correspondingly, the $n^{(j)}$ matrices involved in M' will have the same elements. Hence, there will be at most as many independent elements in M' as are found in a set of non-equivalent groups, namely $(n')^2+(n'')^2+\ \ldots\ +(n^{(k)})^2$. But this number is equal to g (Exercise, § 96). It follows that all these elements are independent, and the theorem is proved.

In the case of the group H of order 6, the matrix M' will have the form (5), § 95, where now

$$a=y_1+y_2+y_3+y_4+y_5+y_6 \qquad b=y_1+y_2+y_3-y_4-y_5-y_6,$$
$$c=y_1+\omega^2 y_2+\omega y_3, \qquad d=y_4+\omega y_5+\omega^2 y_6,$$
$$e=y_4+\omega^2 y_5+\omega y_6, \qquad f=y_1+\omega y_2+\omega^2 y_3.$$

EXERCISES

1. Prove that the n^2 elements of each of the matrices of the transformations of a transitive group G do not satisfy a linear homogeneous equation, whose coefficients are the same for every transformation (Burnside).

2. Prove that if a certain element a_{uv} vanishes in every transformation $S=[a_{st}]$ of a group G, the subscripts u, v being given, then G is not transitive (Maschke).

99. **Theorem 9.** *The number k of non-equivalent transitive linear groups into which the regular group H breaks up* (§ 95) *is equal to the total number of sets of conjugate substitutions of H.* In other words, a given transitive linear group G can be simply or multiply isomorphic with just h non-equivalent transitive linear groups, including

itself and the group consisting solely of the transformation E.

The proof follows that of Theorem 8 closely, after we have first made equal to each other those of the variables $y_1, \ldots, y_g$ which are factors of conjugate transformations in the matrix M. If therefore H contains h conjugate sets of respectively $g_1, \ldots, g_h$ transformations, we shall have h independent variables, say $v_1, \ldots, v_h$.

The matrix M' now has the form of a transformation in canonical form. Thus, the matrix M' in the group of order 6 given in § 95 becomes

$$M' = (a, b, c, c, c, c),$$

where $a = v_1 + 2v_2 + 3v_3$, $b = v_1 + 2v_2 - 3v_3$, $c = v_1 - v_2$. In fact, it follows by Theorem 1, § 89, that, as far as the variables of $H^{(j)}$ are concerned, M' will appear in the form of a similarity-transformation $(\beta_j, \beta_j, \ldots, \beta_j)$, where

$$\beta_j = (g_1 v_1 \chi_1^{(j)} + g_2 v_2 \chi_2^{(j)} + \ldots + g_h v_h \chi_h^{(j)})/n^{(j)}.$$

If $H^{(j)}$ and $H^{(j')}$ are equivalent groups, $\beta_j = \beta_{j'}$; if $H^{(j)}$ and $H^{(f)}$ are non-equivalent, $\beta_j \neq \beta_f$ (cf. § 94, Corollary 1).

Accordingly, among the g multipliers of M' in its new form, there will be just k that are distinct, and these can certainly not furnish more than k expressions linearly independent in $v_1, \ldots, v_h$. On the other hand, the matrix M will contain just h linearly independent elements, namely $v_1, \ldots, v_h$. Hence $k \geqq h$ (cf. proof of Theorem 8), and h of the multipliers $\beta_1, \ldots, \beta_k$ are linearly independent, say $\beta_1, \beta_2, \ldots, \beta_h$. These h expressions can therefore not all vanish unless $v_1 = v_2 = \ldots = v_h = 0$.

However, if $k > h$, the expressions $\beta_1, \ldots, \beta_h$ must all vanish if for $v_1, \ldots, v_h$ we put, respectively, the conjugate-imaginaries of the characteristics $\chi_1^{(h+1)}, \ldots, \chi_h^{(h+1)}$ of the group G_{h+1} (§ 94). But these quantities,

$\bar{\chi}_1^{(h+1)}, \ldots, \bar{\chi}_h^{(h+1)}$ are not all zero (one of them represents the number of variables of $H^{(h+1)}$). We conclude that $k \geqslant h$. Hence, finally, $k = h$.

AN APPLICATION OF THE PRECEDING THEORY

100. **Theorem 10.** *No simple group can be of order $p^a q^b$, p and q being different prime numbers.**

The proof is divided into two parts: (A). If H is the regular substitution group simply isomorphic with a group of order $g = p^a q^b$, assumed simple, then one of the component non-equivalent, transitive linear groups $H', \ldots, H^{(h)}$ contains q^a variables, and one of the conjugate sets of H contains p^β transformations. (B). Under these conditions an impossible equation is derived.

(A). The relation $g = p^a q^b = (n')^2 + (n'')^2 + \ldots + (n^{(h)})^2$ with the conditions that the numbers $n', \ldots, n^{(h)}$ are all factors of g (§ 93, Corollary) and that only one of them is unity (§ 96, Exercise), implies that at least one of them is greater than unity and prime to p; say $n^{(t)} = q^a > 1$.

Again, the relation $g = p^a q^b = g_1 + g_2 + \ldots + g_h$ with the conditions that the numbers $g_1, \ldots, g_h$ are factors of g (§ 29) and that only one of them is unity (or there would be an invariant operator), implies in the same manner that one of them is a power of p; say $g_s = p^\beta > 1$.

(B). We now have a transitive group $H^{(t)}$ in $n^{(t)} = q^a$ variables, and a conjugate set of $g_s = p^\beta$ transformations. Let $S^{(t)}$ denote one of the transformations of this set, $\chi^{(t)}$ its characteristic, and T the corresponding transformation (substitution) of H. We have (§ 90, Exercise 1, and § 133, 7°):

$$p^\beta \chi^{(t)} = q^a K,$$

* Burnside, *Proceedings of the London Mathematical Society*, Series 2, I (1904), 388–92.

where K represents the sum of a finite number of roots of unity. It follows that $\chi^{(t)} = q^a K'$, K' being such a sum also (l.c.). But, $\chi^{(t)}$ is already the sum of q^a roots of unity. Hence, either all these roots are alike, or $\chi^{(t)} = 0$*. The first supposition makes $S^{(t)}$ a similarity-transformation, which would be self-conjugate in $H^{(t)}$. This being impossible for a simple group, we infer that $\chi^{(t)} = 0$; and this not only for the group $H^{(t)}$, but also for every one of the groups $H', \ldots, H^{(h)}$ (and their equivalent groups), the number of whose variables, like $n^{(t)}$, does not contain p as a factor.

Hence, the characteristic of T in H is the expression

$$\chi(T) = n'\chi^{(1)} + \ldots + n^{(h)}\chi^{(h)} = 1 + pK'' + q^a\chi^{(t)} + \ldots = 1 + pK'',$$

when account is taken of the fact that one of the numbers $n', \ldots, n^{(h)}$, say n', is unity, and that the corresponding characteristic $\chi^{(1)} = 1$ (cf. § 95). Accordingly (§ 86, 5°),

$$1 + pK'' = 0.$$

But such an equation is impossible by Kronecker's Theorem (§ 133, 6°). We conclude that H is not simple.

EXERCISE

Prove that a group in which the number of operators in a conjugate set is the power of a prime number, is not simple (Burnside).

*This follows directly from § 133, 6°.

CHAPTER VII

THE LINEAR GROUPS IN FOUR VARIABLES

101. **Introduction.** We shall again adopt all the conventions laid down in § 51, and we shall employ the same classification for the groups now under discussion as that used for the groups in three variables (§ 75). However, we shall begin with the primitive simple groups, the construction of which is the most difficult problem in the present chapter; and, proceeding at a comparatively slower pace while dealing with these groups, we shall determine completely the generating transformations of every type under this head.

On the other hand, there are a host of types of the somewhat more easily constructed groups in four variables which are non-primitive or contain non-primitive invariant subgroups. We shall therefore not attempt to list all of these groups, but shall give an outline of the theory and so much of the detail that the student may encounter no serious trouble in constructing such of these groups as may be needed for any purpose.

The following propositions are of constant use and may be proved by the student (cf. § 31, Exercise 3):

1°. A set of conjugate operators of a group G generate an invariant subgroup of G.

2°. If the generators of G all possess an invariant configuration (function, equation, point, line, plane, etc.), then G will possess the same invariant configuration.

For example, to examine if G is monomial, it is sufficient to try out the generators of G for an invariant set of four planes $X_1X_2X_3X_4=0$. (Cf. § 77, where the solution of this problem is indicated for a group in three variables.)

Again, to examine if G is intransitive or imprimitive in two sets of two variables each (cf. § 120), we write down two sets of two linear functions of the variables with undetermined coefficients: $(a_1x_1+\ .\ .\ +a_4x_4,\ b_1x_1+\ .\ .\ +b_4x_4)$; $(c_1x_1+\ .\ .\ +c_4x_4,\ d_1x_1+\ .\ .\ +d_4x_4)$.

The conditions that each generator of G will transform these sets as sets of intransitivity or imprimitivity will furnish a number of equations among the 16 coefficients a_1 . . that must be simultaneously fulfilled. Thus, if a generator A permutes the two sets, the expressions in the first set are by A transformed into linear functions of the expressions in the second set, and vice versa; that is, certain constants $\lambda_1, \ldots, \mu_4$ can be found such that the following identities in x_1, x_2, x_3, x_4 are fulfilled: $(a_1x_1+\ .\ .)A\equiv\lambda_1(c_1x_1+\ .\ .)+\mu_1(d_1x_1+\ .\ .)$, $(b_1x_1+\ .\ .)A\equiv\lambda_2(c_1x_1+\ .\ .)+\mu_2(d_1x_1+\ .\ .)$; $(c_1x_1+\ .\ .)A\equiv\lambda_3(a_1x_1+\ .\ .)+\mu_3(b_1x_1+\ .\ .)$, $(d_1x_1+\ .\ .)A\equiv\lambda_4(a_1x_1+\ .\ .)+\mu_4(b_1x_1+\ .\ .)$.

It is apparent that the labor involved in a problem of this kind is somewhat tedious, but is not difficult.

Notation.—Throughout this chapter the letters i and ω represent the primitive fourth and third roots of unity, $i=\sqrt{-1}$, $\omega=(-1+i\sqrt{3})/2$, respectively.

Multipliers.—We shall often have occasion to refer to the multipliers or characteristic roots of a transformation (§§ 2, 23). These multipliers are in such cases inclosed in brackets: $[\alpha, \beta, \gamma, \delta]$. Thus, the multipliers of the transformations A_1, A_2, A_3, A_4 of (9), § 123, are all as follows: $[1, 1, -1, -1]$. We call to mind that conjugate transformations have the same multipliers (§ 23); hence if a group G contains a Sylow subgroup of order 7 generated by a transformation whose multipliers are $[1, \beta, \beta^4, \beta^2]$, the multipliers of any transformation in G of order 7 are either $[1, \beta, \beta^4, \beta^2]$ or $[1, \beta^3, \beta^5, \beta^6]$ (§ 36).

Type.—As hitherto, any one of a series of equivalent groups (§ 51, 4°) may be selected as a type of the groups of the series. One group may thus have the type of another group without being written in the same form. For instance, the group (A), § 102, has 10 subgroups all of type (c), § 111, though only one of them has the

canonical form. It also possesses 6 subgroups of type (g), none of which have the monomial form in the variables chosen for (A).

There are in all 30 types of primitive groups in four variables. These types are here designated as follows: (A)–(F),§102; (G)–(K),§119; 1°–7°, §121; 8°–12°, §122; and 13°–21°, §124.

THE PRIMITIVE SIMPLE GROUPS, §§ 102–117

102. **List of the groups.** The groups (A)–(D) are isomorphic with the alternating substitution groups on 5–7 letters: *abcdefg*. The first three are constructed by means of Moore's theorem (§ 50; cf. §§ 58, 82), which gives two solutions for the group of order 60ϕ.* The groups (D)–(F) are obtained in §§ 106–109, 115, 116.

(A) Group of order 60ϕ generated by F_1, F_2, F_3, where

$F_1 = (1, 1, \omega, \omega^2)$;

F_2: $x_1 = \frac{1}{\sqrt{3}}(x_1' + \sqrt{2}x_4')$, $x_2 = \frac{1}{\sqrt{3}}(-x_2' + \sqrt{2}x_3')$,

$x_3 = \frac{1}{\sqrt{3}}(\sqrt{2}x_2' + x_3')$, $x_4 = \frac{1}{\sqrt{3}}(\sqrt{2}x_1' - x_4')$;

F_3: $x_1 = \frac{1}{2}(\sqrt{3}x_1' + x_2')$, $x_2 = \frac{1}{2}(x_1' - \sqrt{3}x_2')$, $x_3 = x_4'$, $x_4 = x_3'$.

The corresponding substitutions of the alternating group are (abc), $(ab)(cd)$, $(ab)(de)$.

(B) Group of order 60 generated by F_1, F_2', F_3', where

$F_1 = (1, 1, \omega, \omega^2)$;

F_2': $x_1 = x_1'$, $x_2 = \frac{1}{3}(-x_2' + 2x_3' + 2x_4')$, $x_3 = \frac{1}{3}(2x_2' - x_3' + 2x_4')$, $x_4 = \frac{1}{3}(2x_2' + 2x_3' - x_4')$;

F_3': $x_1 = \frac{1}{4}(-x_1' + \sqrt{15}x_2')$, $x_2 = \frac{1}{4}(\sqrt{15}x_1' + x_2')$, $x_3 = x_4'$, $x_4 = x_3'$.

* See Maschke, *Mathematische Annalen*, LI (1899), 278–89. A number of the types given by Maschke are intransitive. To obtain the group (D) by Moore's theorem we should have to start with one of these intransitive groups.

(C) Group of order 360ϕ generated by F_1, F_2, F_3 of (A), and F_4: $x_1=x_2'$, $x_2=x_1'$, $x_3=-x_4'$, $x_4=-x_3'$.

The corresponding substitutions of the alternating group are (abc), $(ab)(cd)$, $(ab)(de)$, $(ab)(ef)$.

(D)* Group of order $\frac{1}{2}\cdot 7!\phi=2520\phi$ generated by S, T, W, where

$S=(1, \beta, \beta^4, \beta^2)$;

T: $x_1=x_1'$, $x_2=x_3'$, $x_3=x_4'$, $x_4=x_2'$;

W: $x_1=m(p^2x_1'+x_2'+x_3'+x_4')$, $x_2=m(x_1'-qx_2'-px_3'-px_4')$,

$x_3=m(x_1'-px_2'-qx_3'-px_4')$, $x_4=m(x_1'-px_2'-px_3'-qx_4')$;

where $m=\dfrac{1}{\sqrt{-7}}$, $\beta^7=1$, $p=\beta+\beta^4+\beta^2$, $q=\beta^3+\beta^5+\beta^6$.

The corresponding substitutions of the alternating group are $(abcdefg)$, $(bce)(dgf)$, $(bce)(dfg)$.

(E)† Group of order 168ϕ generated by S, T of (D), and

R: $x_1=n(x_1'+x_2'+x_3'+x_4')$, $x_2=n(2x_1'+sx_2'+tx_3'+ux_4')$,

$x_3=n(2x_1'+tx_2'+ux_3'+sx_4')$, $x_4=n(2x_1'+ux_2'+sx_3'+tx_4')$;

where $n=\dfrac{1}{\sqrt{7}}$, $s=\beta^2+\beta^5$, $t=\beta^3+\beta^4$, $u=\beta+\beta^6$.

(F)‡ Group of order $2^6\cdot 3^4\cdot 5\phi=25920\phi$ generated by T of (D) and C, D, V, F, where

$C=(1, 1, \omega, \omega^2)$; $D=(\omega, \omega, \omega, 1)$;

V: $x_1=x_1'$, $x_2=k(x_2'+x_3'+x_4')$, $x_3=k(x_2'+\omega x_3'+\omega^2x_4')$,

$x_4=k(x_2'+\omega^2x_3'+\omega x_4')$; $k=\dfrac{\omega^2-\omega}{3}=\dfrac{1}{\sqrt{-3}}$;

F: $x_1=-x_3'$, $x_2=x_2'$, $x_3=-x_1'$, $x_4=-x_4'$.

* Cf. Klein, *Mathematische Annalen*, XXVIII (1887), 519; Maschke *ibid.*, LI (1899), p. 291.

† Cf. Maschke, *Papers of the International Mathematical Congress*, Chicago, 1896, p. 176.

‡ Jordan, *Traité des Substitutions*, Paris, 1870, 318; Maschke, *Mathematische Annalen*, XXXIII (1889), 320.

103. **Geometrical properties of transformations of variety 2.** There are two kinds of transformations of variety 2, according to the way in which the multipliers are repeated: $[\alpha, \alpha, \beta, \beta]$ and $[\alpha, \alpha, \alpha, \beta]$.

1°. Interpreting x_1, x_2, x_3, x_4 as homogeneous coordinates of space, a transformation of the first kind, written in canonical form $S=(\alpha, \alpha, \beta, \beta)$, will leave invariant every straight line of the family $ax_1+bx_2=0$, $cx_3+dx_4=0$, where a, b, c, d are arbitrary constants. Correspondingly, there is a family of invariant lines associated with any other transformation T having the same multipliers as S; and since at least one line can always be found belonging to two such families, it follows that S and T have an invariant line in common. If the variables are changed so that this line is $x_1=0$, $x_2=0$, the group H generated by S and T is reducible (x_1 and x_2 being transformed into linear functions of themselves by both S and T). Hence, if S and T belong to a finite group G, the group H is intransitive (§ 20). Let its sets of intransitivity be (x_1, x_2) and (x_3, x_4), and its operators will have the form C_1, § 14. Then if one of the transformations is written in canonical form as far as the variables of any one set are concerned, the corresponding multipliers may be either $[\alpha, \alpha]$, $[\beta, \beta]$, or $[\alpha, \beta]$. In the first two cases S and T are commutative (§ 6, Exercise 2). Accordingly, if they are known not to be commutative, their multipliers must be $[\alpha, \beta]$ for both sets of intransitivity.

2°. The transformation $A=(\alpha, \alpha, \alpha, \beta)$ leaves invariant every plane through the point $x_1=0$, $x_2=0$, $x_3=0$ (namely, every plane whose equation is $px_1+qx_2+rx_3=0$). If B is a transformation having the same multipliers as A, and therefore possessing a similar invariant configuration, the group H generated by A and B must leave invariant every plane through a certain line, namely, the line which joins the two invariant points in question. Moreover, if

A and B belong to a finite group G, and if the variables are so changed that the invariant line is $x_1=0$, $x_2=0$, the group H is intransitive, its sets of intransitivity being (x_1), (x_2), and say (x_3, x_4). As in 1°, the multipliers of A or B corresponding to the intransitive set (x_3, x_4) are $[\alpha, \beta]$, unless A and B are commutative.

Now assume that A and B are of order 5, so that α and β are 5th roots of unity. The component of H in the variables (x_3, x_4), which we shall indicate by H', must then be reducible to the group (E), § 58, by the process of § 12. This group can be generated by the operators of order $2\phi=4$ that it contains; the corresponding operators of H must have the multiplier [1] in the sets (x_1) and (x_2) and will consequently have the multipliers $[i, -i]$ in the set (x_3, x_4) (cf. § 51, 3°). These operators are accordingly of determinant unity in H'; and the group generated by them, namely (E), is therefore a subgroup of H'. Hence, finally, H' contains a transformation of order 3ϕ, whose multipliers are $[-\omega, -\omega^2]$, and correspondingly H contains a transformation whose multipliers are $[1, 1, -\omega, -\omega^2]$ and is not primitive (§ 70).

Next assume A and B two non-commutative conjugate operators under G, of any order. The line $x_1=x_2=0$ invariant under A and B cannot be invariant under every conjugate to A, unless G possesses an invariant intransitive subgroup (§ 101, 1°). Hence assume a conjugate C which does not leave this line invariant. There is, however, an invariant plane common to A, B, C, which passes through the line $x_1=x_2=0$, as is readily seen; and we can so choose the variables that this plane is $x_1=0$. The group K generated by A, B, and C is accordingly intransitive, its sets of intransitivity being (x_1) and (x_2, x_3, x_4). Moreover, the component of K in the variables (x_2, x_3, x_4) is not intransitive by virtue of the assumed facts that A and B generate a transitive group

in (x_3, x_4) and that C does not leave invariant the plane $x_2=0$ (or it would leave invariant the line $x_1=x_2=0$).

EXERCISES

1. Prove that if G contains two non-commutative transformations of order 5, both having the multipliers $[\alpha, \alpha, \beta, \beta]$, and if, furthermore, the intransitive group generated (cf. 1° above) is abelian in one of the sets of intransitivity and not in the other, then G contains a transformation whose multipliers are $[1, 1, -\omega, -\omega^2]$ and is not primitive.

2. If two transformations D and A, whose multipliers are respectively $[\omega, \omega, \omega, 1]$ and $[\alpha_1, \alpha_1, \alpha_2, \alpha_3]$, where $\alpha_1^5=\alpha_2^5=\alpha_3^5=1$, belong to a finite group G, the subgroup generated by them is either abelian or is intransitive in (1, 3) variables. Moreover, the component group in the intransitive set containing 3 variables is again intransitive, since no finite transitive group in 3 variables contains two non-commutative operators of orders 5 and 3 respectively, the latter having the multipliers $[\omega, \omega, 1]$. Hence prove that either the subgroup of G generated by all the conjugates to A is intransitive (all being commutative with D), or that G contains a transformation whose multipliers are $[1, 1, -\omega, -\omega^2]$ and is not primitive.

104. **Theorem 1.** *No primitive simple group G can contain a transformation of order 5 and variety 2.*

Since G can have no invariant subgroup other than itself, a conjugate set of operators of order 5 must generate G (§ 101, 1°). The theorem now follows from § 103, unless every pair of non-commutative conjugate transformations of order 5 and variety 2, having the multipliers $[\alpha, \alpha, \beta, \beta]$, generate an intransitive group H in two sets (x_1, x_2), (x_3, x_4), primitive in both sets.

Consider two such non-commutative transformations, S and T. The two component groups in two variables generated by S and T must each be reducible to the group (E), § 58, by the process of § 12; and it is found that these groups are equivalent, since the generating transformations S and T have the same multipliers $[\alpha, \beta]$

in both sets. An appropriate choice of variables will therefore cause the corresponding matrices to be identical, so that the transformations of H all have the form

$$(1) \qquad \begin{bmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{bmatrix}.$$

It is now easily proved that each line of the family

$$(2) \qquad \lambda x_1+\mu x_3=0, \qquad \lambda x_2+\mu x_4=0,$$

where λ and μ are arbitrary constants, is invariant under H. A similar set of lines will evidently be invariant under the group H' generated by S and a third transformation U having the same multipliers, unless S and U are commutative. Assuming that the variables of G are selected so that S has the canonical form $(\alpha, \beta, \alpha, \beta)$, we find that after a slight reduction the second set of lines can be defined by the equations

$$(3) \qquad \lambda' x_1+\mu' x_3=0, \qquad \lambda'(ax_2+bx_4)+\mu'(cx_2+dx_4)=0,$$

where a, b, c, d are certain constants depending on U, and λ', μ' are arbitrary constants.

The families (2) and (3) are now seen to have at least one line in common, namely, one for which $\lambda=\lambda'$, $\mu=\mu'$, $(\lambda' a+\mu' c)\mu=(\lambda' b+\mu' d)\lambda$. It follows that the group generated by H and H' is reducible and therefore intransitive. Accordingly, any two transformations T and U, both conjugate to S and non-commutative with it, generate with S an intransitive group in two sets of two variables each. This group can be none other than H; hence, all the conjugates to S fall into two classes: those which belong to H, and those which are commutative with S. Any transformation in the latter class must be commutative with every transformation of H, since it

must have the form of a similarity-transformation for each of the two sets of intransitivity: (α, α) in one and (β, β) in the other.

The group generated by S and all its conjugates is therefore either abelian or it contains the intransitive group H as an invariant subgroup. In any event, G is not a primitive simple group.

105. **Theorem 2.** *If a Sylow subgroup P of a simple group G is abelian and contains, aside from the identity, operators of order p only, where p is a prime number, then P is invariant under a larger subgroup Q of G of such a nature that not one of the operators of P except the identity is invariant under Q.*

This theorem is a particular case of a theorem given by the author in *Transactions of the American Mathematical Society*, XI (1910), 2. The proof is long and will not be reproduced here; an outline of the principles involved is given below (§ 107).

106. **Theorem 3.** *The group* (F), § *102, is the only primitive simple group which contains a transformation of order 3 whose multipliers are* $[1, \omega, \omega, \omega]$.*

Proof.—In a group G, let $S_1, S_2, \ldots, S_h$ be a set of conjugate transformations which have the multipliers $[1, \omega, \omega, \omega]$ and which generate an invariant subgroup H. Since G is to be a simple group, we have $H = G$, and H cannot be intransitive by assumption. Hence (§ 103, 2°), we can find three transformations among $S_1, \ldots$ which generate an intransitive group in sets of (1, 3) variables, say (x_1), (x_2, x_3, x_4), while the component group in the variables (x_2, x_3, x_4) is transitive as far as these variables are concerned. Moreover, this component cannot be

* Bagnera, *Rendiconti del Circolo matematico di Palermo*, XIX (1905), 19 ff.

imprimitive since it is generated by transformations having the multipliers $[\omega, \omega, 1]$ (cf. § 86, 5°).

Now, consulting the groups in three variables (chap. v), we discover that only one primitive group possesses operators of order 3ϕ and variety 2, namely, the group (G), § 79, of order 216ϕ. This group may be written as a group K in four variables so that the operators just mentioned (namely, those conjugate to U, § 79) become transformations having the multipliers $[\omega^2, \omega^2, \omega^2, 1]$ in K. The similarity-transformation (ω, ω, ω) in (G) becomes the transformation $(1, \omega, \omega, \omega)$ in K; the latter group is therefore of order $216 \cdot 3 = 648$.

107. A Sylow subgroup P of order 81 is generated by the transformations in K corresponding to S_1, T, U (§§ 77, 79). It contains an invariant abelian subgroup P_1 of order 27, generated by $S_1 = (1, 1, \omega, \omega^2)$, $T^{-1}S_1T = (1, \omega^2, 1, \omega)$, and $U = (\omega^2, \omega^2, \omega^2, 1)$; and it follows from the general theorem referred to in § 105 that G must contain a transformation W_1 which transforms P_1 into itself and which transforms x_1 into a variable different from x_1. The successive steps in the proof of the theorem as applied to the case under consideration are as follows:

1°. The operators of G transform the plane $x_1 = 0$ into a number of distinct planes, say $x_1 = 0$, $x_1' = 0$, $x_1'' = 0$, . . . The geometrical configuration composed of these planes:

$$J \equiv x_1 x_1' x_1'' \ . \ . \ = 0$$

is transformed into itself by G; i.e., J is an invariant of G. Moreover, since G is simple, J must be an absolute invariant (§ 88), since otherwise G is isomorphic with an abelian group in one variable, namely, the variable J.

2°. Now let the planes (factors) in J be separated into sets such that planes of any one set are obtained one from another by operating by the transformations of P_1. The

number of planes in a set is a factor of 27, and the sets do not overlap. If π is a subproduct of J, made up of the factors of a set, then π is an invariant of P_1. From this we find that if π contains only one factor, it is one of the variables x_1 x_2, x_3, x_4. If it contains 3, 9, or 27 factors, then $(\pi)U=\pi$.

3°. The plane $x_1=0$ constitutes a set by itself, and $(x_1)U=\omega^2 x_1$. But, since J is an absolute invariant under G, we must have $(J)U=J$. It follows that there is at least one subproduct π different from x_1 and such that $(\pi)U=c\pi$, where $c\neq 1$. By 2° this factor π is one of the variables x_2, x_3, x_4. Assuming that W was the transformation of G which transformed x_1 into π, we find that the group WP_1W^{-1} leaves $x_1=0$ invariant (viz., $(x_1)WP_1W^{-1}=(\pi)P_1W^{-1}=(c'\pi)W^{-1}=c'x_1$) and will therefore generate with K an intransitive group in (1, 3) variables. However, since (G), § 79, cannot be a subgroup of a larger group in three variables, except one obtained by adding new similarity-transformations, it follows that WP_1W^{-1} is a subgroup of K.

4°. By means of Theorem 7, (*b*), § 36, we can now find a transformation L in K which transforms the Sylow subgroup to which P_1 belongs into the Sylow subgroup to which WP_1W^{-1} belongs. Since a given Sylow subgroup of order 81 contains a single abelian subgroup of order 27, it follows that $L^{-1}P_1L=WP_1W^{-1}$. The transformation LW is now found to possess the properties demanded of W_1 above.

108. The conditions $W_1^{-1}P_1W_1=P_1$, $(x_1)W_1=\pi$, imply that W_1 has the monomial form and transforms x_1 into one of the variables x_2, x_3, x_4, multiplied by a constant. In K we have already the monomial transformations T and V^2 which permute the variables as do the substitutions $(x_1)(x_2x_3x_4)$ and $(x_1)(x_2)(x_3x_4)$ respectively (§ 41). It is therefore possible to multiply W_1 by such a

transformation in the group generated by T and V^2 that this product has the form

F: $x_1 = ax_3'$, $x_2 = bx_2'$, $x_3 = cx_1'$, $x_4 = dx_4'$.

Now, an odd power of F has the same monomial form; we may therefore replace this transformation by such an odd power of itself that the new F is of order 2^n. Furthermore, since $F^2 = (ac, b^2, ac, d^2)$ and is now by assumption of order 2^{n-1}, and since no transformation in canonical form (b^2, ac, d^2) belongs to (G) except such as are of order 3ϕ, it follows that $ac = b^2 = d^2$. In addition, the determinant of F is $-acbd = 1$. Consequently

$$b^4 = \mp 1, \qquad d = \pm b. \tag{4}$$

To determine the coefficients more fully we construct the product FV. Its characteristic is $(b + d\omega)/\sqrt{-3} = b(1-\omega)/3$ or $= b\omega^2$, according as $d = b$ or $= -b$. But $b(1-\omega)/3$ cannot be written as a sum of four roots of unity (§ 86; § 133, 6°) for the values of b satisfying (4). Hence we have $d = -b$; and we may now multiply F by such a power of (i, i, i, i) that we obtain $b = 1$, $d = -1$, $ac = 1$. Finally, the change of variables indicated by the transformation $(-a, 1, 1, 1)$ (cf. § 13) does not alter the group K, while it gives to F the form as listed in the group (F), § 102. Here we have written C and D for S_1 and U^2.

109. The group (F) is evidently primitive (cf. § 101, 2°). Concerning the statement that it is a simple group we merely observe that it is not obtained by enlarging any of the other groups in this chapter. There remains to prove that the transformations T, C, D, V, F actually generate a group of order 25920ϕ. A group of this order cannot be a subgroup of a larger primitive simple group (§ 111); hence no further generators can be added to the list (F).

The 40 planes

$$x_1=0,\ x_2=0,\ x_3=0,\ x_4=0;\ x_2+\theta_1 x_3+\theta_2 x_4=0;$$

$$(5)\qquad x_1-\theta_1 x_2+\theta_2 x_4=0,\ x_1-\theta_1 x_3+\theta_2 x_2=0,$$
$$x_1-\theta_1 x_4+\theta_2 x_3=0;\ (\theta_1,\ \theta_2=1,\ \omega,\ \omega^2),$$

are permuted among themselves by each of the generating transformations given, and therefore by (F) itself. This group is accordingly isomorphic with a (transitive) substitution group on 40 letters, and the order of (F) will be $40k'$, where k' represents the order of that subgroup K' of (F) which leaves $x_1=0$ invariant (§ 45). We now write down a matrix with arbitrary elements $M=[a_{st}]$ to represent a transformation in the group K'. The conditions $(x_1)M=mx_1$, and that M is unitary (§ 19) due to the fact that the Hermitian invariant of (F) can be none other than $x_1\bar{x}_1+x_2\bar{x}_2+x_3\bar{x}_3+x_4\bar{x}_4$, will give us the form C_2, § 14, for M. We finally impose the condition that M permutes among themselves the planes (5); this problem can be simplified by multiplying M by suitable transformations of K. For instance, the case $(x_2)M=m'x_3$ is reduced to the case $(x_2)M=m'x_2$ by substituting MT^{-1} for M at the outset. There results that M belongs to K, so that $K'=K$, and the order of (F) is 25920ϕ.

110. **Theorem 4.** *No primitive simple group can contain a subgroup "H_p"* (§ 66).

Let G be a group which is shown, by application of the theorems of §§ 66–68, to contain an invariant subgroup "H_p". Then since G is here assumed simple, we must have $G=H_p$.

If $p=3$, it follows from § 67 that a transformation T whose order k is prime to 3 must have the multipliers $[1,\ \alpha,\ \alpha,\ \alpha]$; $\alpha^k=1$. But the determinant of this transformation, α^3, cannot be unity. Accordingly, a group H_3 can contain no operator whose order is prime to 3, and is

therefore not primitive (§ 61). Similarly, a group H_p is not primitive if $p>3$.

Consider finally a group H_2. By § 67, a transformation in this group of odd order q must have the multipliers $[\alpha, \alpha, \beta, \beta]$. Therefore, by § 73, $q<6$. Again, by Theorem 1, $q<5$. The order of H_2 is therefore limited to the numbers $2^a \cdot 3^b$, and the group is not simple (§ 100).

111. **The Sylow subgroups.** The theorems of chap. iv and the Theorems 1–4 above enable us to construct, largely by trial, a Sylow subgroup P of order $p^a\phi$ contained in a primitive simple group G. Thus, to construct a group of order $2^a\phi$ we make use of the facts that it can have no transformation of order 8ϕ and variety 4 or 3 (§ 66), and none of order 4ϕ and variety 2. More generally, by following the principles of §§ 66, 68 we may prove that a group in which are present the two commutative transformations $(i, -i, 1, 1)$, $(i, 1, -i, 1)$, either as here written or multiplied by similarity-transformations, must contain an invariant group "H_2". By trial we now find that an abelian group of order $2^4\phi$ will always contain the invariant group "H_2"; hence (§ 74), $a \leqq 3+3=6$.

When $p>3$ the group P is abelian, and Theorem 2, § 105, can be applied. For instance, let us assume a group P of order 7, generated by $S=(1, \beta, \beta, \beta^5)$; $\beta^7=1$. By Theorem 2 there must be an operator T which transforms S into a power of itself: $T^{-1}ST=S^k$, where $k \neq 1$. But no matrix T of non-vanishing determinant exists satisfying the equation $ST=TS^k$. In this manner the various generators of order 7 are excluded except the following: $(1, \beta, \beta^4, \beta^2)$, $(\beta, \beta^6, \beta^2, \beta^5)$, $(\beta^3, \beta^3, \beta^4, \beta^4)$, $(1, 1, \beta, \beta^6)$. But the last two are eliminated by Theorem 8, § 70. Similarly, every abelian group of order 7^2 or 7^3 is eliminated.

The group Q is generally determined by Theorem 2 and § 68. Thus, the cube of the operator T which transforms $S=(1, \beta, \beta^4, \beta^2)$ into a power of itself (say S^2) must be a similarity-transformation. For otherwise we should have a subgroup "H_p," since T^3 is commutative with S. The non-vanishing elements in the matrix of T can now all be made unity by a fitting change of variables and by multiplying T by a power of (i, i, i, i).

In listing the results we use the following abbreviations:

Φ, the group of similarity-transformations contained in G;

P, the Sylow subgroup of order p^a;

Q, that subgroup of G which contains P invariantly, when $p>3$;

T, the transformation $x_1=x_1'$, $x_2=x_3'$, $x_3=x_4'$, $x_4=x_2'$;

R, the transformation $x_1=x_3'$, $x_2=x_4'$, $x_3=x_2'$, $x_4=-x_1'$;

R_1, the transformation $x_1=ax_1'$, $x_2=bx_2'$, $x_3=cx_4'$, $x_4=dx_3'$, where a, b, c, d are certain constants;

V, an operator which permutes among themselves the variables x_3, x_4, and transforms x_1, x_2 into linear functions of themselves;

Q_1, the group of order $m\phi$ generated by all the transformations of G which are not of order $5k$ and which are commutative with the transformation A_1 under (f).

The letters α and β represent respectively primitive 5th and 7th roots of unity; γ, δ, $(\gamma \neq \delta)$, roots of index 11; and ϵ, ζ, $(\epsilon \neq \zeta)$, roots of index 13.

	P:		*Q:*	
Group	Order	Generators	Order	Generators
(a)	$2^a\phi$,	$(a \leqq 6)$;		
(b)	3,	$W' = (\omega, \omega, \omega^2, \omega^2)$;		
(c)	3,	$F_1 = (1, 1, \omega, \omega^2)$;		

		P:	*Q:*	
Group	Order	Generators	Order	Generators
(d)	9,	F_1, $W=(\omega, \omega^2, 1, 1)$;		
(e)	81,	W, T (§ 106);		
(f)	5,	$A_1 \quad =(1, 1, \alpha, \alpha^4)$;	$10m\phi$,	P, Φ, V, Q_1;
(g)	5,	$A_2 \quad =(\alpha, \alpha^4, \alpha^2, \alpha^3)$;	$10m\phi$,	P, Φ, R^2;
(h)	5,	A_2;	20ϕ,	P, Φ, R;
(j)	25,	A_1, $A_3=(1, \alpha, 1, \alpha^4)$;	15ϕ,	P, Φ, T;
(k)	25,	A_1, A_3;	30ϕ,	P, Φ, T, R_1;
(l)	7,	$S \quad =(1, \beta, \beta^4, \beta^2)$;	21ϕ,	P, Φ, T;
(m)	7,	$B \quad =(\beta, \beta^6, \beta^2, \beta^5)$;	14ϕ,	P, Φ, R^2;
(n)	11,	$C \quad =(\gamma, \gamma^{10}, \delta, \delta^{10})$;	22ϕ,	P, Φ, R^2;
(o)	13,	$D_1 \quad =(\epsilon, \epsilon^{12}, \zeta, \zeta^{12})$;	26ϕ,	P, Φ, R^2;
(p)	13,	$D_2 \quad =(1, \epsilon, \epsilon^3, \epsilon^9)$;	39ϕ,	P, Φ, T;
(q)	13,	$D_3 \quad =(\epsilon, \epsilon^{12}, \epsilon^5, \epsilon^8)$;	52ϕ,	P, Φ, R.

It is easy to prove that *no two groups of the types* (e), (f), (j), (k), (l), (m), (n), (o), (p), (q) *can be subgroups of a given group G at the same time.* First, no primitive simple group can contain a transformation whose multipliers are $[\omega, \omega, \omega, 1]$ and at the same time one whose multipliers are those of A_1, by Exercise 2, § 103. Thus the type (e) excludes the types (f), (j), and (k). Secondly, no primitive group can contain a Sylow subgroup of order q and types (l)–(q) and at the same time one of order p or p^2 $(p \neq q)$ and types (e), (f), (j)–(q). For then we should have a transformation U of order pq (§ 90, Cor.), and therefore a transformation of order p (viz., U^q) commutative with one of order q (viz., U^p). But two such transformations would imply a subgroup "H_p," $p \geqq 3$ (§ 68).

Hence, *the order of a primitive simple group in four variables is* $g\phi$, *where* g *is a factor of one of the numbers* $2^6 \cdot 3^4 \cdot 5$, $2^6 \cdot 3^2 \cdot 5^2$, $2^6 \cdot 3^2 \cdot 5 \cdot 7$, $2^6 \cdot 3^2 \cdot 5 \cdot 11$, *or* $2^6 \cdot 3^2 \cdot 5 \cdot 13$.

112. **Reduction in the number of types of the Sylow subgroups.** The types (f), (j), (k), (m), (n), (o), (p), (q)

can be eliminated chiefly by aid of Theorem 4, § 93, from which theorem it follows that if the sum of the products $\chi\bar{\chi}$ exceeds the order $g\phi$ of the group G, then G is intransitive. (For an illustration, the term $\chi\bar{\chi}$ corresponding to the transformation D_2 is $(1+\epsilon+\epsilon^3+\epsilon^9)\ (1+\epsilon^{12}+\epsilon^{10}+\epsilon^4)=3$.)

Consider the type (f). In the group Q there are $5m\phi-m\phi=4m\phi$ transformations whose orders are multiples of 5. Two such transformations belonging to two different subgroups conjugate to Q cannot be identical, since the corresponding transformations of order 5 are distinct. The sum $M=\Sigma\chi\bar{\chi}$ for the transformations of order $5k$ in G will therefore be qh, where q represents the sum of such terms from Q, and h the number of subgroups conjugate to Q, namely, $g\phi/(10m\phi)$, by § 30, Theorem 2′. The group Q is intransitive, in (2, 2) variables: (x_1, x_2), (x_3, x_4); or in (1, 1, 2) variables. Going over the various possibilities in detail we find that the sum q is at least $10m\phi$ (cf. § 94, Exercise 1). The sum M is therefore at least $(g/(10m))\cdot(10m\phi)=g\phi$. But this number, together with the product $\chi\bar{\chi}$ corresponding to the identity, namely, 16, exceeds $g\phi$. In this way the cases (n) and (o) can be disposed of.

113. Consider next the type (m). By § 111 the order of G is in this case a factor of $2^6\cdot3^2\cdot5\cdot7\cdot\phi$. On the supposition that the order is divisible by 5, the group would contain $g\phi/(10\phi)$ or $g\phi/(20\phi)$ subgroups of order 5 (type (g) or (h)), and $g\phi/(14\phi)$ subgroups of order 7. But these numbers should be of the forms $1+5k_1$ and $1+7k_2$ respectively (§ 36). By trial we find this impossible except for the order 210ϕ. But this number does not correspond to a simple group (§ 48). Hence, the order of G is not divisible by 5; and therefore no transitive group isomorphic with G can be constructed in 5 variables (§ 93, Cor.), a fact to be used presently.

Now let G' be a group equivalent to G, differing from the latter merely in being written in the variables y_1, . . , y_4 instead of x_1, . . , x_4. The six functions

$$(6)\quad v_{12}\equiv x_1y_2-x_2y_1,\ v_{13}=x_1y_3-x_3y_1,\ v_{23}=x_2y_3-x_3y_2,\ \ldots,\ v_{34}=x_3y_4-x_4y_3,$$

are readily found to be transformed into linear functions of themselves by the intransitive group made up of G and G' as component groups. We can therefore regard these six functions as the variables of a group H simply isomorphic with G and G'. The transformation B becomes $(1,\ 1,\ \beta,\ \beta^6,\ \beta^3,\ \beta^4)$, and R^2 will permute the variables as indicated in the cycles $(v_{12})(v_{34})(v_{23}v_{14})(v_{24}v_{13})$. By adding the terms $\chi\bar{\chi}$ corresponding to the transformations of order 7ϕ we find that H is intransitive. Hence, since no transitive component can contain 5 variables by what has been proved above, and since no simple group in 2 or 3 variables contains an operator of order 7 which is transformed into its inverse by one of order 2 (viz., R^2), it follows that the components of H are three in number, embracing the variables (v_{12}), (v_{34}), $(v_{23},\ \ldots,\ v_{13})$. In other words, the two functions $v_{12}=x_1y_2-x_2y_1$, $v_{34}=x_3y_4-x_4y_3$, are invariants of H. But it is easily proved that a transformation in four variables whose corresponding operator of H transforms each of these functions into a constant multiple of itself must have the form C_1, § 14. The group G is therefore intransitive.—In the case (q), the group H is first proved to be intransitive in two sets $(v_{12},\ v_{34})$, $(v_{23},\ .\ ,\ v_{13})$, with R permuting the variables in the first set, and with D_3 represented by the identity $(1,\ 1)$ in this set. But no group in two variables $(v_{12},\ v_{34})$, transitive or intransitive, and of order $2n$, can be isomorphic with a simple group of order $52kn$ (cf. § 32). In the case (p), the group H is likewise intransitive, the sets now embracing (3, 3) variables: $(v_{12},\ v_{13},\ v_{14})$,

(v_{23}, v_{34}, v_{41}). But no simple group in three variables is of order $13k$ (cf. chap. v).

114. Finally, assume that the group G contains a group P of type (j) or (k). The order of G is then a factor of $2^6 \cdot 3^2 \cdot 5^2 \cdot \phi$ (§ 111).

Two different subgroups of order 25 cannot have a transformation of order 5 in common. For, let A be a possible common transformation; then, since both groups are abelian, the group generated by them contains A as an invariant transformation and is therefore intransitive. If we now chose for A in turn each of the transformations that belong to P, we find in every case that the sets of intransitivity involve (2, 1, 1) variables. The component group in two variables must be derivable from the group (E), § 58, and G would contain a transformation whose multipliers are $[-\omega, -\omega^2, 1, 1]$ and is not primitive (cf. § 103, 2°).

The total number of Sylow subgroups of order 25 is therefore of the form $1+25k$ (§ 38, Exercise 2). Hence $(1+25k) \cdot 15\phi$ or $(1+25k) \cdot 30\phi$ should be a factor of the order of G (§ 30, Theorem 2′). But this is found to be impossible.

Accordingly, *there remain only the types* (a), (b), (c), (d), (e), (g), (h), *and* (l) *as possible Sylow subgroups of a primitive simple group G in four variables.*

115. **The simple group of order $7 \cdot 9 \cdot k$.** Here we have a group Q of type (l), generated by S, Φ, and T. The last transformation has the multipliers $[1, 1, \omega, \omega^2]$ (cf. § 86, 5°), and belongs to a Sylow subgroup of order 9 and type (d). There is therefore in G a transformation W of order 3 commutative with T, whose multipliers are $[\omega, \omega^2, 1, 1]$. Adopting such variables for G that Q has the form as given under (l), we select a matrix with arbitrary elements to represent W and impose the

conditions that $WT=TW$, and that the characteristics of W, WT, WT^2 are 1, -2, -2 respectively. These conditions determine a matrix with only three arbitrary elements a, b, s:

$$W=\begin{bmatrix} -2-3s & a & a & a \\ b & s+1 & s & s \\ b & s & s+1 & s \\ b & s & s & s+1 \end{bmatrix}.$$

The characteristics of SW and S^3W are $[SW]=-2-3s+(s+1)p$, $[S^3W]=-2-3s+(s+1)q$, where $p=\beta+\beta^4+\beta^2$, $q=\beta^3+\beta^5+\beta^6$; and they are each the sum of the four roots of unity which are the multipliers of the respective transformations. If one of these multipliers is a 7th root of unity or is (more generally) of index $7n$, then the four multipliers are the same as those of S or a power of S, possibly multiplied by a similarity-transformation, since we would otherwise have a subgroup "H_p" (cf. argument at the end of § 111); that is, the corresponding characteristic is $r(1+p)$ or $r(1+q)$, where $r=\pm 1$ or $\pm i$. Kronecker's theorem (§ 133, 6°) can now be applied directly to the equation obtained by eliminating s, and we find the following alternatives:

$$\text{I:}\quad [SW]=-(1+q),\ [S^3W]=-1;$$

$$\text{II:}\quad [SW]=-1,\ [S^3W]=-(1+p).$$

Selecting the first, we derive $s=-(4+p)/7$. Again, from $W^3=E$ we now get $ab=-1/7$; and the change of variables expressed by the transformation $(\sqrt{a/b},\ 1,\ 1,\ 1)$ will finally give us the form of W as written in (D), § 102. The second alternative (II) above would furnish W^2 instead of W.

There remains for us to answer the following questions: Do the transformations S, T, W generate a group of

order $7!\phi/2$, isomorphic with the alternating group on 7 letters? Can no new generators be added to S, T, W? Concerning the first question we remark that if a group G' of order $7!\phi/2$, isomorphic with the alternating group on 7 letters, can be constructed as a linear group in four variables by Moore's theorem (§ 50), then the group generated by S, T, W must be equivalent to G'. For three such operators or their equivalents are evidently present in G'; moreover, the alternating group on 7 letters contains no subgroup of order $63k$ except itself. That the group G' exists has been shown by Maschke (cf. footnote to § 102).

To answer the second question we observe that an assumed primitive simple group generated by S, T, W and additional generators must contain (D) as a subgroup by what precedes, and hence be of order $2^{3+c}\cdot 9\cdot 5\cdot 7\phi$ (§ 111); $c \leqq 3$. Now counting the Sylow subgroups of order 5 and type (h), such groups being already present in (D), and of order 7, we may readily prove that $c=0$ is the only solution (cf. § 113).

116. **The simple group of order $7\cdot 3\cdot k$.** As in § 115, we chose such variables for the group now under discussion (G) that the subgroup Q of order 21 will appear in the form (l), § 111.

In G there is a Sylow subgroup of order 3 generated by T, and the order of G is a factor of $2^6\cdot 3\cdot 5\cdot 7\cdot\phi$. The number of subgroups of order 7 must be either 8 or 64, and correspondingly the order of G is either 168ϕ or 1344ϕ. Only the former number is the order of a simple group (§ 48).

This simple group can be written as a substitution group K on 8 letters *abcdefgh* representing its 8 subgroups of order 21 (§ 46, Cor.). If a represents the group Q, and if S transforms the group b into c, etc., the operators S

and T are in K represented by the substitutions $(bcdefgh)$ and $(cdf)(ehg)$ respectively. An additional generator of G is obtained by constructing an operator R of order 2ϕ, which transforms T into T^2 (§ 105) and whose substitution in K is $(ab)(ch)(de)(fg)$. The conditions $R^{-1}TR=T^2$, $R^2=$a similarity-transformation, give

$$R=\begin{bmatrix} r & v & v & v \\ w & s & t & u \\ w & t & u & s \\ w & u & s & t \end{bmatrix}; \quad r+s+t+u=0^*.$$

We may assume $v=r$; this is equivalent to changing the variables in G by means of the transformation $(v/r, 1, 1, 1)$.

To further specialize the elements in R, we note that with each subgroup of order 21 belongs an invariant plane; in the case of a this is $x_1=0$, the remaining planes being $(x_1)R=0$, $(x_1)RS=0$, . . , $(x_1)RS^6=0$. The planes belonging to c and h are $(x_1)RS\equiv r(x_1+\beta x_2+\beta^4x_3+\beta^2x_4)=0$ and $(x_1)RS^6\equiv r(x_1+\beta^6x_2+\beta^3x_3+\beta^5x_4)=0$; hence, since c is transformed into h by R, we have correspondingly

$$(x_1+\beta x_2+\beta^4x_3+\beta^2x_4)R\equiv k(x_1+\beta^6x_2+\beta^3x_3+\beta^5x_4),$$

where k is an undetermined constant. This condition will fix definitely the ratios of the elements in R; adding the condition that the determinant of R is unity we finally obtain this generator as listed under (E), § 102.

Having proved that no operator except a similarity-transformation can leave invariant each of the 8 invariant planes, we may show that S, T, R generate a group of order 168ϕ, isomorphic with the simple group of order 168 (cf. § 109).

* If $v=0$, the group generated by S, T, R is intransitive.

117. **The simple groups of order 5k.** We come now to the problem of determining the primitive simple groups whose orders are factors of $2^6 \cdot 3^2 \cdot 5 \cdot \phi$, and in which there are subgroups Q of order 10ϕ or 20ϕ as listed under (g) or (h), § 111. Counting the Sylow subgroups of order 5, we discover that the orders of the groups sought are all <1000. Hence, these groups are isomorphic with the alternating groups on 5 and 6 letters (§ 48), and can be constructed by Moore's theorem (§ 50). There result the types (A), (B), (C) (§ 102).

118. **Groups which contain primitive simple groups as invariant subgroups.** In the construction of such groups we are aided materially by the following theorems.

THEOREM 5. *If a given primitive group G does not contain a subgroup "H_p" (§§ 66–68), neither does a larger group K in which G is contained as an invariant subgroup.*

1°. We shall prove that if K contains an invariant subgroup "H_p," then G must contain such a group also. Let H be a subgroup "H_p" of K, and let us assume to begin with that T is an operator common to both G and H and is not a similarity-transformation. If then V belongs to G, the transformation VT belongs to G, and the equation (9), § 66, is true, since it is true when V is any transformation of K and T of H. But if (9) is true, the group G contains an invariant subgroup "H_p" (by the arguments of § 66), contrary to assumption. Hence, G and H can have no operators in common except similarity-transformations.

2°. Now let A be any operator of G, and R of the group H, in K. Then since H is an invariant subgroup, $A^{-1}RA = R_1$ belongs to H. Again, since G is an invariant subgroup, $RAR^{-1} = A_1$ belongs to G. From these two equations we obtain $RA = AR_1 = A_1R$, and therefore

$R_1R^{-1}=A^{-1}A_1$. But R_1R^{-1} belongs to H and $A^{-1}A_1$ to G. It follows by 1° that $R_1R^{-1}=E_1$, a similarity-transformation. Hence, $R_1=E_1R$, so that $A^{-1}RA=E_1R$.

3°. Assuming R not to be a similarity-transformation, let it be written in canonical form, and let A represent in turn every operator of G. We can then prove by the process of § 61 that G is not primitive. Accordingly, since this violates the hypothesis regarding G, the assumption that H is contained in K is untenable.

THEOREM 6. *Let G be a self-conjugate subgroup of K of index h (§ 28) and P a Sylow subgroup of G. Furthermore, let Q and Q' be the largest subgroups of G and K respectively which contain P as an invariant subgroup. Then Q is a subgroup of Q' of index h.*

Proof.—Let $g\phi$ and $gh\phi$ be the orders of G and K; q and q' the orders of Q and Q', and n the number of Sylow subgroups of the same order as P in G. These subgroups form a single conjugate set (§ 36), and therefore $q=(g\phi)/n$. If A is any operator of K, then $A^{-1}PA$ belongs to G and is of the same order as P (§ 30, Exercise 2); the group $A^{-1}PA$ is therefore the group P or another Sylow subgroup conjugate to P. Hence, the n subgroups conjugate to P in G also form a single conjugate set in K, and $q'=(gh\phi)/n$, so that $q'/q=h$. Finally, Q is evidently a subgroup of Q' by the definition of these groups.

119. Now, in the case of the Sylow subgroup (l), the group Q already has the maximum order 21ϕ, barring the existence of an invariant subgroup "H_p". The groups (D) and (E), § 102, can therefore not be contained as invariant subgroups in larger groups. The same argument applies to the group (F), when for P we take a group of order 81, which is already contained in a group Q of order 162 generated by P and V^2.

There remain the groups (A), (B), and (C). Taking for P a subgroup of order 5, the group Q is here of order 10ϕ (type (g), § 111), and may be enlarged to a group Q' of order 20ϕ (type (h)). Hence, these groups (A)–(C) may possibly be enlarged to groups of twice their orders. In fact, the student may verify that the transformation*

$$F': \quad x_1=\psi x_1',\ x_2=\psi x_2',\ x_3=\psi x_4',\ x_4=\psi x_3';\ \psi=\frac{1+i}{\sqrt{2}},$$

does not belong to the group (B), but will transform the generators of (B) in the same manner as the substitution (ab) will transform the corresponding substitutions. Again, the transformation*

$$F'': \quad x_1=x_2',\ x_2=-x_1',\ x_3=x_4',\ x_4=-x_3',$$

does not belong to either (A) or (C), but will transform the generators there listed into new generators in the same way as the substitution (ab) will transform the corresponding substitutions. We therefore obtain three new groups, respectively isomorphic with the symmetric groups on 5, 5, 6 letters, namely,

(G) Group of order 120ϕ generated by (A) and F''.

(H) Group of order 120ϕ generated by (B) and F'.

(K) Group of order 720ϕ generated by (C) and F''.

Evidently none of these new groups can be enlarged.

NON-PRIMITIVE GROUPS AND PRIMITIVE GROUPS WHICH CONTAIN INVARIANT NON-PRIMITIVE SUBGROUPS, §§ 120–125

120. **Intransitive and imprimitive groups.** As remarked in § 101, we shall not present an exhaustive analysis of the remaining groups in four variables. The problems involved are not very difficult, but need on occasion a mass of painstaking labor.

* See Maschke, *Mathematische Annalen*, 1899, referred to in footnote to § 102.

The **intransitive groups** in four variables fall into four classes, according to the number of variables in the different sets of intransitivity, namely, (1, 1, 1, 1), (1, 1, 2), (1, 3), or (2, 2) variables. To construct such a group, say one whose sets of intransitivity involve (2, 2) variables: (x_1, x_2) and (x_3, x_4), we select two transitive binary groups (chap. iii, (B)–(E)) that can be written as isomorphic groups directly or after being enlarged by the method of § 85. To the identity of one group, repeated say k times, will correspond an invariant subgroup of the other of order k (cf. § 32). The transformations of these groups separately need not be of determinant unity (cf. § 51, 2°). Hence, the matrices of the groups (B)–(E) may first be modified by multiplying them by certain similarity-transformations (cf. §§ 10, 12); moreover, operators in the canonical form $(\alpha, \alpha, \beta, \beta)$, where $\alpha^2\beta^2 = 1$, may even be added as new generators.

Imprimitive groups are of two kinds: (*a*) groups which have the monomial form by a proper choice of variables, and (*b*) groups of the form discussed at the opening of § 60. A group G of the first kind (*a*) is isomorphic with one of the transitive substitution groups on four letters, namely, the alternating or symmetric groups on four letters, the Sylow subgroup of order 8 of the symmetric group, or the group (8), § 43. Such a group is therefore of order $12g$, $24g$, $8g$, or $4g$, where g represents the order of the invariant abelian subgroup which has the canonical form when G is written in monomial form. A group of the second kind (*b*) is generated by an invariant intransitive subgroup H and a transformation T which permutes the two sets of intransitivity of H. If the variables are so chosen that the matrices of H have the form C_1, § 14, that of T will have the form of the second matrix given in § 60.

To evaluate the elements of T more definitely we may proceed as follows. The Sylow subgroups of H of order 3^a must be permuted among themselves by T, and since they already constitute a single conjugate set under H, it is possible to find an operator L in H such that the product LT transforms a given Sylow subgroup P into itself (cf. § 107, 4°). Writing P in canonical form, we find that the new T (viz., LT) is a monomial transformation, and we can even make such additional changes in the variables that T has the form $x_1=x_3'$, $x_2=x_4'$, and either $x_3=\alpha x_1'$, $x_4=\beta x_2'$, or $x_3=\alpha x_2'$, $x_4=\beta x_1'$. Moreover, since any odd power of T permutes the two sets of intransitivity of H also, we may assume that originally such a power had been selected that the new T is of order 2^b.

EXERCISE

Prove that either (I), T has the form $x_1=x_3'$, $x_2=x_4'$, $x_3=\alpha x_1'$, $x_4=\alpha x_2'$, or else (II), to the group of similarity-transformations of one of the components of H embracing one set of intransitivity (x_1, x_2) will correspond an invariant subgroup of the other set (x_3, x_4) of order 12ϕ, 24ϕ, or 60ϕ. (Hint: construct T^2 and $T^{-1}PT$, belonging to H, and make use of the facts that none of the groups (C)–(E), chap. iii, have a transformation of order 2ϕ commutative with one of order 3ϕ; and also that if H contains a transformation whose multipliers are $[\theta, \theta, \rho\omega, \rho\omega^2]$ and is of order ϕ in the variables (x_1, x_2) and of order 3ϕ in the variables (x_3, x_4), then (II) is true.)

121. **Primitive groups having invariant intransitive subgroups.*** It is easily proved that if a primitive group G contains an invariant intransitive subgroup H, none of the sets of intransitivity can embrace just one variable (cf. method of proving the lemma, § 61). The transformations of H must therefore have the form of

* Goursat has determined all the groups in four variables which leave invariant the quadric $x_1x_4-x_2x_3=0$. These include all the groups enumerated in this and the following paragraph. See "Sur les substitutions orthogonales, etc.," *Annales scientifiques de l'École Normale Supérieure*, (3), VI (1889), pp. 62–79.

C_1, § 14, and the two straight lines $x_1=x_2=0$, $x_3=x_4=0$ are invariant under H. If these are the only invariant lines, G will be intransitive or imprimitive, since a line which is invariant under H is by an operator of G transformed into a line also invariant under H. We therefore assume at least one additional invariant line; this can be written $x_1+x_3=0$, $x_2+x_4=0$ by a suitable choice of variables. The matrices of H are then seen to have the form of the matrix (1), § 104.

All the lines invariant under H now belong to the family (2), § 104, and are, as remarked, permuted by G. In order that this condition may be fulfilled, the matrices of G must necessarily have the form

$$(7) \qquad \begin{bmatrix} pt & pu & qt & qu \\ pv & pw & qv & qw \\ rt & ru & st & su \\ rv & rw & sv & sw \end{bmatrix}.$$

The numbers $p, q, \ldots, w$ in the different transformations of G are readily determined from the fact that

$$A_1=\begin{bmatrix} p & q \\ r & s \end{bmatrix}, \qquad A_2=\begin{bmatrix} t & u \\ v & w \end{bmatrix}$$

are corresponding matrices of two groups, say G_1 and G_2, in two variables, simply isomorphic with G. (This we discover when we multiply together two transformations of the form (7)). Moreover, G_1 and G_2 may simultaneously be given any convenient forms, independently of each other, that would be obtainable through separate changes of variables. They must both be primitive, and are therefore to be selected from the groups (C)–(E), chap. iii. For if, say, G_2 were imprimitive, we could write it in monomial form; the group G would then appear as an intransitive or imprimitive group.

To the group of similarity-transformations in G_1 will correspond an invariant subgroup H_2 of G_2, and vice versa. The group H_2 is transitive, since it includes a component of H. Hence, if G_2 is of order 12ϕ, H_2 is of order 4ϕ (generated by W_1 and W_3, § 57) or of order 12ϕ; if the order of G_2 is 24ϕ, that of H_2 is 4ϕ, 12ϕ, or 24ϕ; finally, if the order of G_2 is 60ϕ, that of H_2 is 60ϕ. Setting up an isomorphism with the primitive group G_1, we find the orders of the respective groups as follows:

	1°	2°	1°	2°	3°	4°	5°	6°	7°
H_1:	4ϕ	4ϕ	12ϕ	12ϕ	12ϕ	12ϕ	24ϕ	24ϕ	60ϕ
G_1:	12ϕ	24ϕ	12ϕ	24ϕ	12ϕ	12ϕ	24ϕ	24ϕ	60ϕ
H_2:	4ϕ	4ϕ	12ϕ	12ϕ	24ϕ	60ϕ	24ϕ	60ϕ	60ϕ
G_2:	12ϕ	24ϕ	12ϕ	24ϕ	24ϕ	60ϕ	24ϕ	60ϕ	60ϕ
G:	48ϕ	96ϕ	144ϕ	288ϕ	288ϕ	720ϕ	576ϕ	1440ϕ	3600ϕ

The groups 1° and 2° are monomial, while the groups 1°–7° are all primitive. No new types are obtained by interchanging the subscripts 1 and 2 in 3°, 4°, or 6°, since the groups so derived are equivalent to the original groups.

The primitive groups 1°–7° leave invariant the quadric surface $x_1x_4-x_2x_3=0$, and this one only. The family (2), § 104, constitutes one of the two systems of straight lines lying upon this surface; the other is $\xi x_1+\eta x_2=0$, $\xi x_3+\eta x_4=0$.

122. **Groups containing as invariant subgroups the primitive groups of § 121.** An operator which leaves invariant each of the two families of lines lying on the quadric $x_1x_4-x_2x_3=0$ will have the form (7); one which interchanges them will have the form

$$(8) \qquad \begin{bmatrix} pt & qt & pu & qu \\ pv & qv & pw & qw \\ rt & st & ru & su \\ rv & sv & rw & sw \end{bmatrix}.$$

New groups, different from those already listed in § 121, can therefore be obtained only by including a transformation T of the form (8) among the generators of the groups 1°–7°. This operator will transform H_1 into H_2 and vice versa; the orders of H_1 and H_2 are therefore equal, and we are limited to the cases 1°, 2°, 5°, and 7°.

The order of T may be assumed a power of 2 (cf. argument at the end of § 120). Under this assumption it is contained in a Sylow subgroup P of order 2^{a+1} (§ 39), namely, the group generated by T and the Sylow subgroup of G of order 2^a which is transformed into itself by T. Writing P in monomial form, we find that for T may be chosen a generator which permutes the variables in the order $(x_1)(x_2x_3)(x_4)$, say

$$T: \quad x_1=\alpha x_1', \quad x_2=\beta x_3', \quad x_3=\gamma x_2', \quad x_4=\delta x_4' \qquad (\alpha\delta=\beta\gamma).$$

Now consider a group generated by T and the group 2°. The groups H_1 and H_2 being given as in § 57, (C), the conditions that T^2 belongs to G and that $T^{-1}H_1T=H_2$, are now found to be equivalent to the equations $\alpha^4=\beta^4=\gamma^4=\delta^4$. But since the change of variables indicated by the transformation $(1, 1, i, i)$ produces the operators of G over again in the same forms (though not in the same order), we may introduce this change (if necessary) in T so as to obtain $\alpha^2=\beta^2$. Again, if $\alpha=-\beta$, we may replace T by the product WT, where W belongs to P and has the canonical form $(1, -1, 1, -1)$; if $\alpha=-\gamma$, we replace T by TW. Hence, finally, we have the two possibilities:

$$T_1: \quad \alpha=\beta=\gamma=\delta=\frac{1+i}{\sqrt{2}}; \qquad T_2: \quad \alpha=\beta=1, \ \gamma=\delta=i.$$

There result two groups, 8° and 9°, both of order 576ϕ, generated respectively by 2° and T_1, 2° and T_2.

The transformation T_2^2 is not contained in either 1° or 7°. Hence we here obtain only one new group in each

case, 10° and 11°, of orders 288ϕ and 7200ϕ, generated respectively by 1° and T_1, 7° and T_1.

Finally, the group 5° already contains the transformation $R=(1, 1, i, i)=T_2T_1^{-1}$. The groups generated by 5° and T_1 or by 5° and T_2 are accordingly identical, furnishing a single new group, 12°, of order 1152ϕ.

EXERCISES

1. The primitive groups 1°–12° all leave invariant the surface $x_1x_4-x_2x_3=0$, and only this one of the second degree. Prove that any operator which transforms this surface into itself must have the form (7) or the form (8). Hence prove that a group which contains self-conjugately any one of the groups 1°–12° is already included in this list.

2. The groups 1°–12° and the group (B), § 102, are the only primitive groups in four variables which leave invariant a quadric surface. In the case of the group (B), this surface has for equation $x_1^2+x_2^2+2x_3x_4=0$, which can be transformed into the equation $z_1z_4-z_2z_3=0$ by the following change of variables: $x_1=z_2+z_3$, $x_2=i(-z_2+z_3)$, $x_3=-z_1$, $x_4=2z_4$. Introduce this change in (B) and compare the new generators with the matrix (7).

123. **Primitive groups having invariant imprimitive subgroups.** In the study of these groups the following proposition is found useful:

Given a group G and a positive integer n. The group generated by the nth powers of the operators of G or of an invariant subgroup of G is again an invariant subgroup of G. (The method of proof is embodied in Exercise 3, § 31.) It should be noted that the group generated by the nth powers of the *operators* of G is not necessarily the group generated by the nth powers of the *generators* of G.

Now consider a group G which contains invariantly an imprimitive subgroup K of the kind classified under (*b*), § 120. The group generated by the second powers of the operators of K is intransitive, and therefore G is found among the groups defined in § 121. The only exception

is furnished by a group K the second powers of whose operators all reduce to similarity-transformations. In such a case K must be of order $2^m\phi$ and can therefore be written in monomial form. We find by trial that it is of order 16ϕ and is generated by the transformations

$$A_1=(1,\ 1,\ -1,\ -1), \qquad A_2=(1,\ -1,\ -1,\ 1)$$

$$(9)\quad A_3=\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \qquad A_4=\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

to which may be added the similarity-transformation (i, i, i, i).

Next let K belong to the class (a), § 120, at the outset. The cases where K is of order $4g$ or $8g$ come under the class of groups mentioned above; there remain the cases where K permutes the variables in the same way as the alternating or the symmetric groups on four letters. The latter case is reduced to the former by taking for a new K the group generated by the second powers of the transformations of K as given. Again, when K corresponds to the alternating group, it is reduced to a monomial group of order $4g$ by taking the group generated by the third powers of its transformations.

Hence, finally, our problem is limited to that of finding the primitive groups which contain the group (9) self-conjugately.

124. **The group F of order 11520ϕ isomorphic with the symmetric group on 6 letters.*** Referring to § 113, let G and G' be equivalent groups in $x_1, \ldots$ and $y_1, \ldots$, and H the isomorphic group in the six variables (6):

* Klein, *Mathematische Annalen*, II (1870), 198 ff.; IV (1871), 356; Maschke, *ibid.*, XXX (1887), 496 ff.

$v_{12}, \ldots, v_{34}$. If we in the latter group change the variables to $w_1, \ldots, w_6$, where

$$(10) \quad \begin{array}{lll} w_1 = v_{12} + v_{34}, & w_3 = v_{13} + v_{42}, & w_5 = v_{14} + v_{23}, \\ w_2 = v_{12} + v_{43}, & w_4 = v_{13} + v_{24}, & w_6 = v_{14} + v_{32}, \end{array}$$

the group (9) will have taken the canonical form and be of variety 6. Accordingly, H will permute among themselves the six variables $w_1, \ldots, w_6$ (cf. § 61).

The following statements may now be proved by the student:

(*a*) A transformation of G whose corresponding transformation of H has the canonical form must belong to K.

(*b*) Consequently, if two transformations of H permute $w_1, \ldots, w_6$ in the same way, one of the two corresponding transformations of G is equal to the other multiplied by a transformation of K.

(*c*) Now, the transformations:

$$S = \frac{1+i}{\sqrt{2}}(i, i, 1, 1), \quad T = \frac{1+i}{2}\begin{bmatrix} -i & 0 & 0 & i \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & -i & i & 0 \end{bmatrix}$$

permute the variables $w_1, \ldots, w_6$ in the orders $(w_1 w_2)$ and $(w_2 w_4 w_6 w_3 w_5)$ respectively, and will therefore with K generate a group F of order $16 \cdot 720 \cdot \phi$, isomorphic with the symmetric group on the six letters $w_1, \ldots, w_6$. By (*a*) and (*b*), this group will contain every transformation which leaves K invariant.

(*d*) Hence, finally, all the primitive groups which contain K as an invariant subgroup are contained as subgroups in the group F.

(*e*) Now, any two subgroups, F_1 and F_2, are equivalent when their corresponding substitution groups, F_1' and F_2', on the letters $w_1, \ldots, w_6$ are conjugate under the symmetric group of order 720. For, if a substitution

transforms F_1' into F_2', the corresponding operator of F will transform F_1 into F_2. Hence, to determine all the primitive, non-equivalent subgroups of F, we first select a representative of each set of conjugate subgroups of the symmetric group under discussion. Every such representative of order $5k$ will furnish a primitive group, since the linear group generated by K and T is primitive (§ 101). There are in all 9 groups of order $5k$:

Group	Order	Generating Substitutions	Generating Transformations
13°	$5\cdot 16\phi$	$(w_2w_4w_6w_3w_5)$;	K, T;
14°	$10\cdot 16\phi$	" $(w_3w_6)(w_4w_5)$;	K, T, R^2;
15°	$20\cdot 16\phi$	" $(w_3w_4w_6w_5)$;	K, T, R;
16°	$60\cdot 16\phi$	" $(w_3w_4)(w_5w_6)$;	K, T, SB;
17°	"	" $(w_1w_2)(w_3w_6)$;	K, T, BR;
18°	$120\cdot 16\phi$	" (w_5w_6);	K, T, A;
19°	"	" $(w_1w_2)(w_3w_4)$ (w_5w_6);	K, T, B;
20°	$360\cdot 16\phi$	" $(w_1w_2)(w_3w_4)$;	K, T, AB;
21°	$720\cdot 16\phi$	" (w_1w_2);	K, T, S.

Here $A=\rho(1, i, i, 1)$, $B=\rho(1, 1, 1, -1)$, where $\rho=(1+i)/\sqrt{2}$; and R is the transformation: $x_1=\frac{1}{\sqrt{2}}(x_1'+ix_2')$, $x_2=\frac{1}{\sqrt{2}}(ix_1'+x_2')$, $x_3=\frac{1}{\sqrt{2}}(ix_3'+x_4')$, $x_4=\frac{1}{\sqrt{2}}(-x_3'-ix_4')$.

125. There are no more primitive groups. For a subgroup F_1' of the symmetric group on six letters contains an invariant subgroup F_2' of order either 2, 4, 3, or 9, unless the order of F_1' is a multiple of 5. If F_2' is of order 2 or 4, the corresponding subgroup F_2 of F is of order 32ϕ or 64ϕ, and the group F_1 containing F_2 invariantly belongs to the category of groups discussed in § 121 (cf. § 123). If F_2' is of order 3, it is generated by $(w_3w_6w_4)$ or by $(w_1w_3w_5)(w_2w_4w_6)$. In the first case, F_1 contains a self-conjugate

intransitive subgroup, namely, one generated by the second powers of F_2 (the transformation corresponding to $(w_3w_6w_4)$ is $BR\cdot AB$ and has the form of C_1, § 14). In the second case, F_2 is generated by K and the transformation $x_1=x_1'$, $x_2=x_3'$, $x_3=x_4'$, $x_4=x_2'$, and F_1 by F_2 and the transformations B and SR^2, corresponding to (w_1w_2) (w_3w_4) (w_5w_6) and (w_1w_2) (w_3w_6) (w_4w_5), or is a subgroup of this group, excepting the possibility where the order of F_1 is divisible by 9, treated below. But this group is monomial. Finally, if F_2' is of order 9, the corresponding subgroup F_2 of F must be equivalent to the group 1°, § 121, both having an invariant subgroup of order 16ϕ, equivalent to K, and both being of the same order (§ 124, (d)). Hence, F_1 must be one of the groups 1°–12°.

In conclusion, we point out that no new groups arise by enlarging any of the groups 13°–21°. For each of these groups contains a single invariant subgroup of order 16ϕ, namely, K. This is readily seen when we observe that no subgroup of order 2^a of the symmetric group on the letters $w_1, \ldots, w_6$ can be transformed into itself by $T=(w_2w_4w_6w_3w_5)$. Accordingly, a group which contains one of the groups 13°–21° self-conjugately must therefore also contain K self-conjugately, and is again one of the groups 13°–21°.

CHAPTER VIII

ON THE HISTORY AND APPLICATIONS OF LINEAR GROUPS*

126. The theory of linear groups of finite order may be said to have been originated by F. Klein, who in 1876 constructed the binary linear groups in order to solve a certain problem in the Theory of Invariants.† Subsequently he extended the Galois Theory of Algebraic Equations by the introduction of linear groups‡ (cf. § 127).

An important problem connected with Linear Differential Equations, namely the determination of those equations of this type whose coefficients are rational functions of the independent variable x and whose solutions are algebraic functions of x, was in the meantime attacked by various men, in particular H. A. Schwarz,§ L. Fuchs,‖ and C. Jordan.¶ Their solutions hinged upon the discovery of the invariants of certain corresponding linear groups or the groups themselves, although the group-notion was not at first introduced, except by Jordan. This author made the problem entirely one of linear

* In the matter of references, the following abbreviations are used in the present chapter: *Annalen*, 2, 9, 12, 28, 50, 52, 60, 71, for *Mathematische Annalen*, Bd. 2 (1870), 9 (1876), 12 (1877,) 28 (1887), 50 (1898), 52 (1899), 60 (1905), 71 (1912), respectively; *Crelle*, 75, 81, 84, 85, for *Journal für die reine und angewandte Mathematik*, Bd. 75 (1873), 81 (1876), 84 (1878), 85 (1878), respectively; *Transactions*, VI, VIII, XIV, for *Transactions of the American Mathematical Society*, VI (1905), VIII (1907), XIV (1913); *Icosaeder*, for *Vorlesungen über das Icosaeder*, by F. Klein, Leipzig, 1884; *Valentiner*, for *De endclige Transformations-Gruppers Theori*, Videnskabernes Selskabs Skrifter, (6), Copenhagen, 1889.

† *Annalen*, 9, pp. 183–208.

‡ Cf. *Icosaeder*.

§ *Crelle*, 75, pp. 292–335.

‖ *Ibid.*, 81, pp. 97–142; 85, pp. 1–25.

¶ *Ibid.*, 84, pp. 89–215.

groups; and, having proved a proposition concerning the order of such groups (§ 74), he was able to state a general theorem about the degree of the algebraic equation whose roots satisfy a linear differential equation (cf. § 128).*

Having briefly mentioned the important applications of linear groups, outside of general group-theory proper, we shall give a survey of the progress of the theory up to the present. As already stated, Klein began by the construction of the groups in two variables. This was followed by different determinations of the same groups by P. Gordan, Jordan, and H. Valentiner,† and of the groups in three variables by Jordan‡ and Valentiner§. A general theory for any number of variables was outlined by the former and applied by him with partial success to the groups in four variables.‖ In addition, special groups of the latter category that arose in analysis, or special classes of such groups, were discussed by other mathematicians (Klein,¶ Goursat,** Bagnera,†† etc.). The complete determination of the groups in four variables (aside from intransitive and monomial types) was carried through by the author.‡‡ More recently, H. H. Mitchell has given a partial determination of these groups by means of a classification based upon certain geometrical properties.§§

There are, in the main, four distinct principles employed in the determination of the groups in 2, 3, or 4

* *Ibid.*, p. 91.

† See footnote to § 52.

‡ *Crelle*, 84, pp. 125–215.

§ *Valentiner* (cf. footnote above).

‖ *Atti della Reale Accademia della Scienze fisiche e matematiche di Napoli*, t. 8 (1879).

¶ *Annalen*, 2, pp. 198 ff.; 28, pp. 504 ff., etc.

** *Annales scientifiques del'Ecole Normale Supérieure* (3), t. 6 (1889), pp. 9–102.

†† *Rendiconti del Circolo Matematico di Palermo*, t. 15 (1901), 161–309; t. 19 (1905), pp. 1–56.

‡‡ *Annalen*, 60, pp. 204–31; *Transactions*, 6, pp. 232–36.

§§ *Transactions*, 14, pp. 123–42.

variables: (*a*) the original geometrical process of Klein (chap. iii); (*b*) the processes leading to a diophantine equation, which may be approached analytically (Jordan, § 59), or geometrically (Valentiner, Bagnera, Mitchell); (*c*) a process involving the relative geometrical properties of transformations which represent "homologies" and like forms (Valentiner, Bagnera, Mitchell; cf. §§ 80, 103); (*d*) a process developed from the properties of the multipliers of the transformations, which are roots of unity (Blichfeldt, §§ 63–68). A new principle has been added recently by Bieberbach, though it had already been used by Valentiner in a certain form (see footnote p. 97).*

Independent of these principles stands the theory of group characteristics, of which G. Frobenius is the discoverer (chap. vi). Important additions have been made by I. Schur, W. Burnside, and T. Molien.† Recently L. E. Dickson has developed a theory of group characteristics for modular groups.‡

In conclusion we shall dwell for a moment on an important question connected with linear groups: What is the arithmetical nature of the elements involved in such groups? The following theorem has been established (Maschke,§ Burnside,‖ Schur¶): "The n variables may be so chosen that every element in the matrices is a cyclotomic number (that is, a linear function of roots of unity with coefficients which are rational numbers). Possible exceptions to this rule can occur only if the

* The author has amplified this principle and hopes shortly to publish his results (cf. § 74).

† See footnote to § 84.

‡ *Transactions*, 8, pp. 389–398; *Bulletin of the American Mathematical Society* (2), XIII (1907), 477–88.

§ *Annalen*, 50, pp. 492–98.

‖ *Proceedings of the London Mathematical Society*, (2), III (1905), 239.

¶ *Sitzungsberichte der Königl.-Preuss. Akademie der Wissenschaften*, 1906, pp. 164 ff.

characteristic equation $(-\theta)^n+A(-\theta)^{n-1}+ \ . \ . \ . \ =0$ (§ 23) of every transformation of the group has the form of a perfect kth power, k being greater than unity and a factor of n." In addition, Schur has proved that the elements are algebraic integers (§ 134), when the variables are suitably chosen.* In the case of a monomial group, W. A. Manning has demonstrated that under a proper choice of variables, every non-zero element is a root of unity.†

127. We shall now outline briefly the main points in the Galois theory of equations and Klein's extension thereof.‡ Let $A\equiv x^n-c_1x^{n-1}+c_2x^{n-2}- \ . \ . \ =0$ be an equation whose coefficients $c_1, \ . \ . \ , \ c_n$ are numbers in a domain R. (A *domain* R consists of all numbers which are rational functions with rational coefficients of certain specified numbers $k_1, \ . \ . \ , \ k_m$ defining R; for instance, the domain defined by a single rational number k, different from zero, is the aggregate of all rational numbers, including zero.) The equation $A=0$ is *irreducible* in R if A is irreducible; that is, if no factor of A exists which is a polynomial in x of degree $<n$ and with coefficients in R. Under this condition, integers $m_1, \ . \ . \ , \ m_n$ can be found such that the $n!$ expressions $y_1, \ . \ . \ y_{n!}$, obtained from $y_1=m_1x_1+ \ . \ . \ +m_nx_n$ by subjecting $x_1, \ . \ . \ , \ x_n$ to all the $n!$ possible permutations, are all distinct. Consider the function $B\equiv(y-y_1)(y-y_2) \ . \ . \ . \ (y-y_{n!})$. The coefficients of the different powers of y are all symmetric functions of $x_1, \ . \ . \ , \ x_n$ and are therefore numbers in R. Let $B'\equiv(y-y_1)(y-y_2) \ . \ . \ . \ (y-y_g)$ be a factor of B, irreducible in R; the equation $B'=0$ is called a *Galoisian resolvent* of $A=0$ for the domain R. Its roots $y_1, \ . \ . \ , \ y_g$ are obtained from one of them by subjecting $x_1, \ . \ . \ , \ x_n$

* *Annalen*, 71, p. 365.

† *Bulletin of the American Mathematical Society* (2), XII (1905), 77–79.

‡ Cf. Miller, Blichfeldt, and Dickson, *Theory and Applications of Finite Groups*, New York, 1916, pp. 279 ff.

to g substitutions forming a substitution group G, called *the group of the equation* $A=0$ for the domain R. Then, according to the Galois theory, if a rational function of the roots $x_1, \ldots, x_n$ with coefficients in R (or in an enlarged domain R' containing R) is an absolute invariant under G, this function equals a number in R (or R'). Again, if G has an invariant subgroup of index p (a prime number), the resolvent $B'=0$ can be broken up into factors by the "adjunction" to our domain R of the roots of unity of index p (i.e., including these roots among the defining numbers of the domain), as well as a radical $\sqrt[p]{K}$, where K is a number in the enlarged domain R.

In Klein's theory, we construct the regular substitution group H of order g consisting of the permutations that take place among the roots of $B'=0$ when $x_1, \ldots, x_n$ are subjected to the substitutions of G. This group H is intransitive as a linear group (§ 96), breaking up into component groups $H', H'', \ldots$, of respectively $n', n'', \ldots$ variables, linear functions of $y_1, \ldots, y_g$. At least one of the numbers $n', n'', \ldots$ is unity (say $n'=1$), the corresponding variable being $y_1+y_2+\ldots+y_g$. If H contains an invariant subgroup of index p (a prime number), then an additional number $n'', \ldots$ is unity, say $n''=1$. The corresponding variable is of the form $Y\equiv y'+\theta y''+\ldots+\theta^{p-1}y^{(p-1)}$, where θ is a root of unity of index p, and $y', y'', \ldots$ are each the sum of g/p of the letters $y_1, \ldots, y_g$. The transformations of H'' are here of the form $Y=\theta^j Y'$, so that $Y^p=K$ is an absolute invariant of H'' and therefore also of H and G. In agreement with the Galois theory, K is a number in the domain R' obtained by adjoining θ to R, and we have $Y=\sqrt[p]{K}$.

On the other hand, if H is simple, then none of the numbers $n'', \ldots$ equals unity. Consider in this case the group H'' in n'' variables. Its invariants are invariants of H and G, and are, accordingly, equal to numbers

in the domain R'' obtained by adjoining to R those coefficients of the various products of $x_1, \ldots, x_n$ involved in the invariants in question which are not already numbers of R (these coefficients depend only on the integers $m_1, \ldots, m_n$ and the "multiplication table" of the group H and are *presumably* "cyclotomic" numbers; cf. §§ 95, 126). If therefore we are able to evaluate, in some way, the n'' variables of H'' from these invariants, we shall have obtained that many new unsymmetrical functions of the roots of $A=0$, and our problem has been reduced correspondingly. This evaluation is what is called the *binary, ternary,* etc., *form-problem,* in the cases $n''=2, 3,$ etc. The form-problem of the first order ($n''=1$) is solved by the extraction of a radical ($\sqrt[p]{K}$), and an equation can be "solved by radicals" if the form-problems of the successive resolvents are all of the first order.

Consider the "general" quintic equation

$$A \equiv x^5 - c_1 x^4 + \ldots = 0.$$

If the numbers defining the domain R be the coefficients $c_1, \ldots, c_5$ and the square root of the discriminant of $A=0$, the group of this equation becomes the alternating group on 5 letters. The numbers $n'', \ldots,$ corresponding to the different non-equivalent groups $H'', \ldots$ are 3, 3, 4, 5 (cf. Exercise 1, § 97). The general quintic can accordingly be reduced by means of a ternary form-problem. But, if the equation $A=0$ is first thrown into the form $A' \equiv v^5 + av^2 + bv + c = 0$ by means of the so-called Tschirnhausen transformation (requiring the extraction of a square root in addition to rational operations performed on the coefficients $c_1, \ldots, c_5$), its reduction is made to depend upon a binary form-problem. For, the 60 functions obtained by permuting the roots $v_1, v_2, \ldots, v_5$ of $A'=0$, according to the alternating group on 5 letters, in the function

$$z_1 \equiv (v_1 + v_2\theta + v_3\theta^2 + v_4\theta^3 + v_5\theta^4)/(v_1 + v_2\theta^2 + v_3\theta^4 + v_4\theta + v_5\theta^3),$$

where θ is a fifth root of unity, are all linear fractional functions of z_1 (when account is taken of the relations $v_1+\ .\ .\ +v_5=v_1v_2+\ .\ .\ +v_4v_5=0$):

$$z_s=\frac{p_sz_1+q_s}{r_sz_1+t_s} \qquad (s=1,\ 2,\ .\ .\ .,\ 60),$$

namely the functions representing the 60 transformations of the linear fractional group (§ 11) corresponding to the binary icosahedral group (E), § 58 (second form). The invariants of this group are accordingly equal to numbers in the domain defined by θ, the coefficients of $A'=0$, and the square root of the discriminant of $A'=0$.

Extending these results, Klein has made the reduction of the general equations of degrees 6 and 7 depend upon a ternary and quaternary form-problem respectively, the corresponding linear groups being the *Valentiner group* of order 360ϕ* and a group of order $7!\phi/2$ in four variables first constructed by Klein.† Beyond that, the general equation of degree $n\geqq 8$ can be reduced by a form-problem of order $n-1$, but not lower (Wiman‡).

128. The application of linear groups to linear differential equations having algebraic solutions will now be briefly explained. By the "domain R" should here be understood the aggregate of all constants (real or complex, algebraic or transcendental) and all rational functions of a single complex variable x, and by an "algebraic function of x" shall be meant a function which is a root of an algebraic equation whose coefficients are functions in R.

Consider the differential equation ($y'=\frac{dy}{dx}$, etc.):

$$y''+py'+qy=0, \tag{1}$$

where p and q are functions in R. Let it be given that the equation is "irreducible" in R (i.e., no solution of

* *Valentiner* (cf. footnote at the opening of § 126), p. 198; the group is (I), § 82.

† *Annalen*, 28, p. 519. ‡ *Ibid.*, 52, p. 243.

(1) satisfies an equation $y'+ry=0$, where r is in R), and also that two independent solutions y_1, y_2 of (1) are algebraic functions of x. Then if s is an arbitrary constant (not specified), the function

$$v_1=\frac{sy_1'+y_2'}{sy_1+y_2}$$

is a solution of the differential equation

$$v'+v^2+pv+q=0, \tag{2}$$

and is at the same time a root of an algebraic equation

$$v^m+A_1v^{m-1}+\ \ldots\ +A_m=0, \tag{3}$$

with coefficients A_1, . . . in R. If we assume that (3) is irreducible in R, it follows that its roots are all solutions of (2). Hence, any such root must be of the form

$$v_2=(s'y_1'+y_2')/(s'y_1+y_2),$$

where s' is a constant. On the other hand, the roots of (3) are all of the form v_1 as regards s; it is therefore easy to prove that $s=(as'+b)/(cs'+d)$, where a, b, c, d are certain (known) constants. But this is the typical form of a linear fractional transformation T_2, and we may write $(v_1)T_2=v_2$.

The roots of (3) are accordingly obtained from v_1 by subjecting s to m linear fractional transformations $T_1, \ldots, T_m$. It is readily seen that these transformations form a group G. For, writing s' originally instead of s in v_1, the roots of (3) would evidently again be derived from the new form of v_1 (which is the original v_2) by subjecting s' to the same linear fractional transformations $T_1, \ldots, T_m$. Accordingly, the products T_2T_1, $T_2^2, \ldots, T_2T_m$ are $T_1, \ldots, T_m$ over again in some order.

It follows that m is one of the numbers g, $2g$, 12, 24, 60 (cf. §§ 11, 56–58). However, s can be specialized so as to reduce this number m. For, let G contain a subgroup H of order h, which possesses a linear invariant when it is written as a linear group in two "variables" s, t; by a suitable choice of these variables we can cause this invariant to be t. If then we put $s=0$ in (3), the resulting equation will have h roots all equal to y_2'/y_2, and (3) will break up into h equal factors. Omitting the case $m/h=1$, we finally find that the degree of the equation (3) may be put equal to 2, 4, 6, 12, in the cases where the "monodromie" groups are the linear fractional groups corresponding to (B), (C), (D), (E), §§ 56–58, respectively.

Similar results are obtained for linear differential equations of any order. In the case of an irreducible linear homogeneous differential equation of the third order, whose coefficients are in R and whose solutions are algebraic, the degree of the algebraic equation with coefficients in R satisfied by the function y'/y of a certain solution y of the differential equation, is 3, 6, 6, 9, 9, 6, 36, 21, according as the corresponding linear fractional group is isomorphic with the linear group (C), . . , or (J), §§ 76, 79, 82. This is Jordan's theorem (cf. § 126), as modified by adopting Painlevé's substitution ($v=y'/y$).*

The complete determination of the types of equations (1) whose monodromic group is the icosahedral group (E), § 58, has been carried through by Klein, chiefly by aid of the "Schwarzian derivative": $y'''/y'-\frac{3}{2}(y''/y')^2$, which remains unaltered when y is subjected to a linear fractional transformation with constant coefficients.† Similar methods have been applied to the equations of the third order by Painlevé* and Boulanger.‡

* *Comptes rendus*, Paris, 104 (1887), pp. 1829–32; *ibid.*, 105 (1888), pp. 58–61.

† *Annalen*, 12, pp. 167–80.

‡ *Journal de l'Ecole Polytechnique* (2), 4 (1898), pp. 1–122.

APPENDIX

129. **Congruences.** The symbol

$$A \equiv B \pmod{k} \tag{1}$$

is read "A is congruent to B modulo k" and takes the place of the equation

$$A = B + Ck$$

where C is a positive or negative integer or zero. The congruence is used in preference to the equation whenever it is immaterial just what the value of C is. The following rules apply: if $A \equiv B$ and $C \equiv D \pmod{k}$, then

$$\begin{aligned} A - B &\equiv 0 \pmod{k}, \\ mA &\equiv mB \pmod{k} \text{ when } m \text{ is an integer}, \\ A \pm C &\equiv B \pm D \pmod{k}, \\ AC &\equiv BD \pmod{k}. \end{aligned}$$

The least absolute remainder (positive or negative) obtained when a number A is divided by k is called the *remainder of* A *(mod* k*)*.

Remark.—In chap. iv, the congruence notation (1) is extended to the case where A and B are sums of roots of unity, the meaning now being that "A equals $B \pm k \times$(the sum of a finite number of roots of unity)."

130. **Roots of a congruence.** Let a, b, c be given integers and p a prime number, then by "a root of the congruence"

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

is meant such an integer (if any) which, when substituted for x, will cause the left-hand member to become an integral multiple (positive or negative) of p, or zero.

For example, the congruence $x^2-1\equiv 0 \pmod 2$ has for root every odd number. These are all $\equiv 1 \pmod 2$; we therefore say that the congruence given has just one root (mod 2). If $p>2$, the congruence $x^2-1\equiv 0 \pmod p$ has two roots (namely ± 1). The congruence $x^2\equiv 2 \pmod 3$ has none.

We have the following theorem:

A congruence of the n^{th} degree ($ax^n+\ \ldots\ \equiv 0$) has at most n roots (mod p), p being a prime number.

131. **Indeterminate equations of the first degree.** The congruence

$$ax\equiv c \pmod b$$

is equivalent to the *indeterminate equation*

$$ax+by=c,$$

to be satisfied by integral values of x and y.

If the highest common factor of a and b divides c, there is always a solution of this equation. In particular, if $c=1$, there is a solution if a and b are prime to each other.

132. **On a certain class of determinants.** The determinant

$$f(x_1, \ldots, x_n)=\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ x_1^2 & x_2^2 & \ldots & x_n^2 \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix}$$

has the value

$$f=(x_2-x_1)(x_3-x_1)\ \ldots\ (x_n-x_1)\cdot(x_3-x_2)\ \ldots\ (x_n-x_2)\cdot\ \ldots\ (x_n-x_{n-1}),$$

and is a factor of the determinant

$$F \equiv \begin{vmatrix} x_1^a & x_2^a & \dots & x_n^a \\ x_1^b & x_2^b & \dots & x_n^b \\ \dots & \dots & \dots & \dots \\ x_1^m & x_2^m & \dots & x_n^m \end{vmatrix}.$$

The value of the quotient F/f, when $x_1, \dots, x_n$ all have been replaced by 1, may be found by treating the fraction F/f as an "indeterminate form 0/0." We put $x_1 = 1$ and let x_2 approach 1 as a limit; the value of F/f will then become

$$\left(\frac{\delta F}{\delta x_2} \Big/ \frac{\delta f}{\delta x_2}\right)_{x_1 = x_2 = 1}.$$

Next we let x_3 approach 1, etc. The final result is the ratio of the two following determinants:

$$D = \begin{vmatrix} 1 & a & a(a-1) & a(a-1)(a-2) & \dots \\ 1 & b & b(b-1) & b(b-1)(b-2) & \dots \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 1 & m & m(m-1) & m(m-1)(m-2) & \dots \end{vmatrix},$$

$$\begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 1 & 0 & \dots & 0 \\ 1 & 2 & 2! & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & n-1 & (n-1)(n-2) & \dots & (n-1)! \end{vmatrix};$$

namely $D : [2!\ 3!\ \dots\ (n-1)!]$

We find

$$D = \begin{vmatrix} 1 & a & a^2 & \dots \\ 1 & b & b^2 & \dots \\ \dots & \dots & \dots & \dots \\ 1 & m & m^2 & \dots \end{vmatrix} = f(a, b, \dots, m).$$

133. **On roots of unity.** A solution of the equation

$$x^n = 1,$$

n being a positive integer, is called a *root of unity.* A solution α is in particular called a *primitive* n^{th} root of unity, if n is the least integer for which $\alpha^n = 1$. In such a case n is called the *index* of the root.

The following theorems are useful:

1°. The product or ratio of two roots of unity is a root of unity.

2°. Any positive or negative rational power of a root of unity is again a root of unity.

3°. If n is the index of a root α, and m a positive integer, the index of α^m is n/d, where d is the highest common factor of n and m.

4°. If the index of a root θ is $n = ab$, where a and b are two integers which are prime to each other, then it is possible to find a root of index a, say α, and one of index b, say β, such that $\theta = \alpha\beta$.

As is customary, we write ω, ω^2 for the roots of index 3, and i, $-i$ for the roots of index 4.

5°. If α is a root of index n, then the n solutions of $x^n = 1$ are $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, and we have

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{n-1} = 0$$

6°. *Theorem of Kronecker.**—For the proper handling of a certain class of equations a very effective theorem due to Kronecker is necessary. We shall not make a formal statement of the theorem, but explain its meaning by implication.

The class of equations referred to are all of the form $\sum_{j=1}^{k} a_j = 0$, $a_1, \ldots, a_k$ being roots of unity, and the

* "Mémoires sur les facteurs irréductibles de l'expression $x^n - 1$," *Journal de Mathématique pures et appliquées*, I, t. 19 (1854), pp. 178 ff.

question involved is this: If we know nothing about these roots except their number k, what can be inferred concerning their values? Kronecker's theorem implies that the k roots fall into sets, each containing a prime number of roots the sum of which equals zero. Moreover, if p is the number of roots in any one set, and if a is a root of index p, then the roots of the set are ϵ, ϵa, ϵa^2, . . . , ϵa^{p-1}, where ϵ is an unknown root of unity. We shall discuss in full the cases $k=3, 4, 5$.

$k=3$: $a_1+a_2+a_3=0$. Here we have $a_2=a_1\omega$, $a_3=a_1\omega^2$.

$k=4$: $a_1+a_2+a_3+a_4=0$. We have two sets of two roots each, say $a_1+a_2=0$, $a_3+a_4=0$.

$k=5$: $a_1+a_2+a_3+a_4+a_5=0$. There are two possibilities: one set only, or two sets containing 3 and 2 roots respectively. If β represents a primitive 5th root, and γ, δ roots of unknown indices, the two cases are respectively given by

$$\gamma+\gamma\beta+\gamma\beta^2+\gamma\beta^3+\gamma\beta^4=0;$$
$$(\gamma-\gamma)+(\delta+\delta\omega+\delta\omega^2)=0.$$

By means of Kronecker's theorem the following can be proved:

7°. If N represents the sum of a finite number of roots of unity and k an integer, and if it be known that N/k is an *algebraic integer* (§ 134), then N/k equals the sum of a finite number of roots of unity.

More definitely, the roots in N can be arranged in two sets such that the sum of those in one set vanishes and those in the other set are each repeated k (or a multiple of k) times.

8°. By *Demoivre's Theorem:*

$$(\cos\theta+i\sin\theta)^n=\cos n\theta+i\sin n\theta,$$

the roots of unity of index n can be expressed in the form

$$\alpha^m = \cos\frac{m}{n}\,360° + i\,\sin\frac{m}{n}\,360°,$$

where m represents in turn every integer prime to and less than n.

The conjugate-imaginary of α^m is accordingly α^{-m}.

134. **On algebraic integers.** An *algebraic integer* is a number which satisfies an equation of the form

$$x^n + a_1 x^{n-1} + \ . \ . \ + a_{n-1}x + a_n = 0,$$

where $a_1, \ . \ . \ , a_n$ are positive or negative integers or zero.

If α and β are algebraic integers, and k an ordinary integer, then $\alpha+\beta$, $\alpha\beta$, and $k\alpha$ are algebraic integers.

If a/b is an algebraic integer, and at the same time a and b are ordinary integers, then a/b must be an ordinary integer.

INDEXES

GENERAL INDEX

[Numbers refer to pages]

INDEX OF AUTHORS

[Numbers refer to pages]